Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.

The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

<table>
<thead>
<tr>
<th>FRCC</th>
<th>Florida Reliability Coordinating Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRO</td>
<td>Midwest Reliability Organization</td>
</tr>
<tr>
<td>NPCC</td>
<td>Northeast Power Coordinating Council</td>
</tr>
<tr>
<td>RF</td>
<td>ReliabilityFirst</td>
</tr>
<tr>
<td>SERC</td>
<td>SERC Reliability Corporation</td>
</tr>
<tr>
<td>SPP RE</td>
<td>Southwest Power Pool Regional Entity</td>
</tr>
<tr>
<td>Texas RE</td>
<td>Texas Reliability Entity</td>
</tr>
<tr>
<td>WECC</td>
<td>Western Electricity Coordinating Council</td>
</tr>
</tbody>
</table>
Preamble

In November of 2016 the ERO published a list of Reliability Risk Priorities developed from recommendations made by the Reliability Issues Steering Committee to the NERC Board of Trustees. The document included a list of Risk Profiles that reflect the top priorities of the industry, one of which is Risk Profile #8: Physical Security Vulnerabilities. This risk profile states the possibility that the intentional damage, destruction, or disruption to facilities can cause localized to extensive interconnection-wide BPS disruption potentially for extended periods.

This guideline document has been developed by the Critical Infrastructure Protection Committee (CIPC) to provide guidance for electric system entities in assessing physical security vulnerabilities in accordance with the risk defined in Risk Profile #8.

The content of this guideline document is not intended to establish new requirements, modify existing requirements, nor provide interpretation of existing standards or requirements.
Introduction

The nature and magnitude of extreme events pose an immediate and serious risk to an entity’s ability to effectively fulfill its responsibilities to the BPS operation, support, and control. In an environment where customer dependency on reliable electric service is critical and where physical attacks are expected to increase, it is increasingly important that practical and objective assessments be performed and their findings acted upon.

This guideline will focus on the development of resiliency and physical security vulnerability assessment best practices and planning as would be necessary to mitigate extreme events rather than addressing details of the response to such an event.

This guideline has been developed to focus on assessment of vulnerabilities that have the potential to result in events that would fall in the High Impact quadrants of the graphic below, primarily the upper left High Impact Low Frequency category.

![Impact/frequency matrix](image)

**Figure 1.1** Impact/frequency matrix.

The graphic below further demonstrates the need for continuous monitoring and review for events that fall within quadrants 1 and 2 which result in Very High or Extreme consequences.
**Figure 1.2** Likelihood vs. Consequence matrix
Chapter 1: Scope

The goal of this guide is to identify and promote specific resiliency and vulnerability assessment best practices with planning for extreme events, including best physical security assessment practices, as shown in Item 7.(a) of the Recommendations for Mitigating the Risk section of Risk Profile #8.

Identified risks as listed in Risk Profile #8 are:

1. The increasing and evolving threat around physical attacks.
2. The exposed nature of the grid, which is vulnerable and difficult to protect.
3. Long lead times associated with manufacturing and replacing some equipment, which can increase complexity of restoration after physical attacks that damage BPS equipment.
4. The level of industry knowledge or coordination in accessing the existing spare equipment inventory.
5. Physical damage to generation fuel sources, such as natural gas pipelines, which will degrade the reliable operations of the BPS.
6. Damage to long-haul telecommunications and water supplies, which will make certain critical facilities vulnerable and reduce the ability to serve load.
7. An EMP event, which could lead to widespread loss of load in certain regions.

Physical security risks and the effects of those risks are ever present and should be assessed and planned for in any vulnerability assessment. However, the planning for an event that occurs on an extraordinary scale or escalates from a relatively minor event to an extreme event requires a planning model that is robust and capable of adapting to the current situation and conditions as the event matures.

Various factors contribute to the magnitude and scope of an event and its classification as an extreme event. When performing assessments and planning for extreme events it is important to consider that events may not be and may not appear to be extreme events when first recognized, but at some point, due to conditions surrounding the event, escalate to ‘extreme’ status.

Events may quickly escalate into extreme events depending on: 1.) The level of the impact. If the event is confined to a local facility the impact to the BPS is likely minor and the response localized, however if the event is regional or national the impact will be more significant. 2.) The entities level of preparedness. An entity who has made no preparation may struggle in its response as compared to an entity that has a mature plan with effective mitigation measures ready to deploy. 3.) The level of resources necessary to effectively respond to an event can also have an effect on the success of the response, and finally 4.) The possibility of a cascading effect into BES assets or other critical infrastructure sectors can result in the escalation of an ordinary event.
Chapter 2: Planning for Extreme Events

This guideline presupposes that your company emergency response plans and security measures capture most of the elements required for the tactical response to what we view as extreme events. The purpose of this section is to discuss the strategic elements that your organization will require to respond to extreme or catastrophic events.

When developing your plan, start with a consideration of your organization’s priorities. Knowing your priorities will help you determine the resilience and recovery options you should be considering. The following are some areas to consider to help guide your discussions:

- Virtually every organization counts the safety of employees, contractors, visitors, and members of the public as a priority, and the electricity sector is no different. Everything is replaceable except for human life. Your response to an extreme event should reflect this, above all, care for people first.

- Protection of the environment - Damaging the environment affects others and can have consequences that can threaten your ability to operate, so you must ensure that environmental protection is considered in all planning.

- Physical asset protection - Physical and cyber assets are necessary to generating, transmitting, and distributing electricity or any other product. Damage to assets can keep your company out of the marketplace for a long time, so should be addressed early.

- Restoration of service - Safe and secure operations depend on other factors, such as people, and properly functioning equipment.

The elements of response at this level are as follows:

- **Crisis Management Team** - for assessing damage, marshalling information and resources, ensuring the safety and survival of employees, and protecting the public. This team will manage the crisis using the priorities stated earlier as a guide. The Director of the Crisis Management Team should be a Senior Executive (or equivalent).

- **External Liaison and Notification** – Is this an event which will overwhelm an organization’s capability to adequately respond, so external resources will need to be brought in? Are there regulatory reporting requirements that need to be addressed? Do neighboring facilities need to be informed?

- **Communications Plan** - (both external and internal (including the Board of Directors), and including social media policies, employee notification, and employee contact information)

- **Restoration Team** - a subset of the Crisis Management Team, this group works to prepare the organization for a return to the ‘new normal.’ This team will include operations, supply chain, finance, HR, and Security.

**Security Planning**

Security planning for extreme events should be part of the Crisis Management Team suite of plans, as it will be executed under its supervision.
## Chapter 2: Planning for Extreme Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Priority</th>
<th>Function</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Bomb attack    | Safety   | • Emergency response plans for all aspects related to bombs: bomb threats reporting, premises searches, suspicious package protocol, response to explosions (evac, etc.)  
• Training and equipping employee First Aid teams | Most of the activities in this area are found in the domain of emergency response planning and the corporate safety management program. |
| Prioritizing Communications |                      | • Strict social media policy (no unauthorized tweeting or Facebook posts during emergency events)  
• Corporate communications plan to promote employee and public notification in the event of an emergency | A response to an extreme event may be disrupted by family or media pressure. Good communications planning can help to prevent this, but ensuring that your employees know why it is important not to put photographs on social media, and the consequences if they do, will help the communications effort. |
| Physical Asset Protection |                      | • Access control to prevent unauthorized persons from entering facility  
• Bollards to keep vehicles back from inhabited buildings | Planning for a bomb attack starts during the design phase of physical security measures. If the original design did not include measures needed during a bomb threat, then temporary measures can be introduced until the permanent measures are installed. For example, a truck or Jersey barriers can be used to block a road to prevent vehicle access until bollards are installed. |
| Restoration of Service |                      | • Business Continuity Plans | Business Continuity Plans which allow for the loss of production, administrative office space, information systems, or personnel are needed here. |
Chapter 3: Vulnerability Assessments

A vulnerability assessment is an examination of an entity’s asset(s) to identify conditions that might be exploited or attacked by an attacker to cause harm to the asset or the people associated with the asset.

It may be helpful to recall how NIST defines Vulnerability Assessment for information systems:

“Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.” (Source: NIST NIST.SP.800-30r1)

Similarly, a physical security vulnerability assessment would include a comprehensive review of the physical security posture with the purpose of identifying as many vulnerabilities as possible. Vulnerabilities being weaknesses that can be exploited by a threat source. It would entail a comprehensive review for the purposes of identifying, quantifying and prioritizing the vulnerabilities at an asset or with related personnel to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

A vulnerability assessment requires you to try to see your own physical security faults as an attacker would see them. Such an assessment is sometimes difficult to do effectively due to cognitive biases. ([https://en.wikipedia.org/wiki/Cognitive_bias](https://en.wikipedia.org/wiki/Cognitive_bias)). Following an extreme event, consideration should be given to whether to request assistance from an outsider to validate an existing vulnerability assessment or conduct a new vulnerability assessment.

After an extreme event has occurred, a vulnerability assessment should be created if it does not exist or updated with the current situation if it does exist.

While in a defensive role, you need to think like those in an offensive role. Questions to ask would include when, where and how would an attacker attack this target or the people employed here. Essentially, you are performing a target assessment. A vulnerability assessment looks for and finds the weaknesses in processes, locations, structures, materials, and devices that security and facility managers would normally (and mistakenly) rely on to provide a secure environment.

The vulnerability assessment may bring to light areas in which the extreme event has caused either a degradation or loss of functionality in a security measure. The incapacity to perform as designed could be exploited by a threat actor or in some cases may be the intended consequence of the threat actor as a step towards additional second or third order effects. The assessment may lead to the identification of additional or adaptive security measures.

When creating or updating a vulnerability assessment it is useful to start with a list of the assets to be protected and the identified threats. In an extreme event, the list of assets should be reviewed to determine the order of priority in which the vulnerability assessment is conducted. The identified threats may have changed significantly during an extreme event and should be reviewed.
For each asset, the vulnerability assessment should give consideration to the following factors:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Asset (structure) design</td>
<td>Features of the asset design that create weakness that can be exploited by an adversary, such as open areas allowing operations to be observed from the outside, etc...</td>
</tr>
<tr>
<td>Proximity to uncontrolled areas</td>
<td>Areas that are not controlled by your company especially areas allowing public assess for travel or occupation</td>
</tr>
<tr>
<td>Portals</td>
<td>Entry points into the asset by vehicles or people</td>
</tr>
<tr>
<td>Barriers</td>
<td>Obstacles such as fences, walls, gates or environmental features.</td>
</tr>
<tr>
<td>Access by uncleared personnel</td>
<td>Access by people who have not undergone your company credentialing process including escorted access.</td>
</tr>
<tr>
<td>Access by required services</td>
<td>Access by people such as deliveries, utilities or emergency services.</td>
</tr>
<tr>
<td>Area denied to access</td>
<td>Identified areas where vehicles or people are not allowed.</td>
</tr>
<tr>
<td>Areas minimized to access</td>
<td>Identified areas where access is restricted, such as to company vehicles or employees only.</td>
</tr>
</tbody>
</table>

Each factor should be scrutinized to determine any security faults that could be exploited by an attacker. Example questions for each factor would include:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Sample Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Asset (structure) design</td>
<td>How could surveillance be conducted? How are the materials used to construct the asset? How susceptible is the asset to an explosion? What are the blast zones based off a Design Basis Threat? How susceptible is the asset to gunfire? What internal and external lighting options are available? What materials were used for walls, floors, ceilings and roofs? What are the asset external penetrations?</td>
</tr>
<tr>
<td>Proximity to uncontrolled areas</td>
<td>How close can the public get to the asset? What of the asset can be seen from public spaces? What are the ingress and egress points to observation locations? Is there a public parking lot or parking garage close to the site? Is there a public use trail or park close to the site?</td>
</tr>
<tr>
<td>Portals</td>
<td>How many and where are the vehicle entry points? How many and were are the people entry points? What mechanism prevents or slows access at the entry points? What mechanism detects or logs access at the entry points? Are there trenches, ducts, sewers, storm drains allowing access? Are there railroad tracks or pipelines entering the perimeter? Are there straight-line vehicle approaches to critical areas?</td>
</tr>
<tr>
<td>Barriers</td>
<td>What creates the physical security perimeter for the asset? Is there a layered approach to the barriers? What are the barriers constructed from? Does the terrain help or hinder an attacker? What vegetation is present? Are barriers fixed or moveable?</td>
</tr>
<tr>
<td>Access by uncleared personnel</td>
<td>How do people get access to the asset?</td>
</tr>
</tbody>
</table>
| Access by required services | Who approves access?  
Who escorts and how many can be escorted at one time?  
Is there a visitor access program?  
Is there an established stand-off zone for vehicles? |
|----------------------------|--------------------------------------------------|
| Access by required services | How do outside service people access the site?  
Are vehicles searched upon entry or exit?  
How do you verify the service person is legitimate?  
Are escorts needed for some services versus others?  
Are deliveries confined to a certain area?  
Who approves service people to enter the asset? |
| Area denied to access | Are there areas that foot traffic is not allowed?  
Are there areas that vehicle traffic is not allowed?  
What are the protection methods for the areas?  
Is there an established exclusive stand-off zone? |
| Areas minimized to access | Are there areas that only certain foot traffic is not allowed?  
Are there areas that only certain vehicle traffic is not allowed?  
What are the protection methods for the areas? |

One of the fundamental questions for each factor is whether the extreme event has altered the security protections in place for that factor.
Chapter 4: Physical Security Assessments

In order for an entity to evaluate the effectiveness of its physical security measures, a periodic assessment of those measures is appropriate. In preparation for events that may be extreme or escalate to extreme status assessments are crucial in order to respond effectively.

Physical security baseline – Before preparing for extreme events, the following physical security practices should be applied to the current state of physical security. Critical assets should be identified based on industry regulations (ex.: NERC Critical Infrastructure Protection Reliability Standards) and enterprise business continuity requirements. Classification levels should be given to assets based on their level of criticality (ex.: level 1 for the lowest level of criticality and level 4 for highest level).

Minimum physical security measures should be implemented based on the level of criticality (ex.: Level 1 can be mechanical access control and Level 4 can be two-factor authentication (2FA) electronic access control with IDS perimeter system and on-site response force). Also, there should be an escalation of measures added to the minimum based on the threat of extreme events or history of victimization.

Assessment audits which focus on physical security measures such as evaluation of perimeter integrity and use of physical security measures by employees should be performed at a frequency determined by the level of criticality of the asset. (ex.: level 1 should be audited once a year and level 4 once a month) Reporting of any security events and physical security vulnerabilities by employees and contractors to the security department should be mandatory (ex.: breach in fencing, door that doesn’t lock properly, loss of access card, etc.).

Physical security assessment should be done on all assets that are required to protect (generating station, substation, control center, data centers, transmission lines, etc.) and considered as a normal business good practice. Updates on the assessments should be made when any change occurs in operations or configuration of an asset that can have an impact on the physical security measure effectiveness.

Description of physical security assessment¹- A security survey should be a thorough, on-site examination, the purpose of which is to: 1.) Determine and document the current security posture, and how might that posture change if an extreme event is imminent, 2.) Identify deficiencies and excesses in existing security measures, 3.) Evaluate the current posture with a determination of appropriate level of security or protection needed and recommend improvements in the overall situation.

Physical security assessment for planned extreme events - Identify levels of threats (anticipated or real) for extreme events that you can plan ahead of and consider physical security measures to add to or modify your baseline for each level. Integrate your physical security measures to existing business continuity plans. Adjust physical security measures baseline to the level of threat. The physical security measures baseline should be adjusted whether the threat is anticipated or real. Consider adopting a Spare equipment / Mobile equipment strategy to improve your resiliency.

¹ Based on extracts of Physical Security Principles, ASIS, 2015
Physical security assessment for unplanned (ex.: active shooter) extreme events - Identify your contingencies for your physical security measures baseline – Example: lockdown policies and physical security measures for active shooter situations. Prepare your contingencies to be able to deploy them when extreme events occur – Example: rehearse lockdown procedure with security personnel once a year at critical locations. Identify any gaps (situation that you don’t have any contingency for) and assess the risk. If the risk is not acceptable, close the gap by adding the appropriate measures. Consider improving system redundancy. – Example – if you do not physical security measures to permit lockdown procedures for your employees, evaluate the risk of active shooter situations for your assets and based on risk evaluation, either accept the risk or implement measures to permit lockdown procedure.
Chapter 5: Drill & Exercises

This section covers the facet of preparation for an extreme event. The nature of extreme events is to be unforeseen and likely impossible to be prepared for. Emergency managers must design their programs to maintain readiness for all hazards as defined per both National Incident Management System (NIMS) and the Incident Command System’s all hazards approach. Additionally, those who assume the role of Emergency Manager are responsible for preparing and evaluating their entities ability to respond and recover from extreme events.

Preparation and evaluation are critical for maintaining operational resilience. Facing disasters with unevaluated emergency plans often results in poor procedural execution, leading to confusion in response and recovery. Currently, OSHA standards 1910.38 suggest an expectation that entities conduct drills and exercises to evaluate an entity’s performance towards site level emergencies. These scenarios are based on situations likely to occur within the workplace, such as active shooter, fire drill or other emergencies. Additional consideration shall be made towards planning drills and exercises that evaluate preparation for extreme events.

The Framework

The overwhelming and unpredictability of an extreme event may immediately deplete resources directed towards the initial response. Extreme events will likely be an event with both an expansive footprint and/or intensifying levels of complexity. Unlike low-level site events involving site management, and local first responders; extreme events involve a large group of first responders, technical experts from private organizations and government agencies. The entity’s emergency management program should have a framework or system in place to facilitate the rapid increase of personnel.

Entities conduct exercises to evaluate the performance of their individual business units. Exercising for extreme events presents entities with opportunities to test current framework. Results of these exercises provide entities the opportunity to identify challenges associated with implementation and logistics necessary to accommodate these additional responding agencies. Throughout history, the challenges identified in responding to large scale events like Hurricane Katrina have involved problems with command and control, resource distribution and prioritization of response. Due to the nature of extreme events, the Incident Command System provides a framework allowing agencies to streamline capabilities to adjoin with multiple agencies and jurisdictions during an event.

Exercising the Framework

The objective of drills and exercises is to evaluate the capabilities of a program. Drills are defined as coordinated supervised activities, usually employed to test a single operation or function within an entity. Drills are designed to review the performance of smaller sections of a larger group. Most drills are performed shortly after the initial instruction of a task or procedure. Drills are presented as opportunities for participants to ask questions and receive correctional guidance during the performance of actions.

There are three forms of exercises. The first is the functional exercise (FE), which examines and/or validates the coordination, command and control between various multi-agency coordination centers. FEs are most common, as they utilize minimal involvement from personnel and resources. During these exercises department resources and involvement by other agencies can be simulated. The second form of exercise is the full-scale exercise (FSE) designed to display coordination between multi-agency, multi-jurisdictional, multi-disciplinary resources intended to facilitate
a functional organizational response, where personnel and resources are implemented in real time. Entities are encouraged to conduct FSE’s every 2-3 years to prevent strain on resources.

Finally, the best practice in exercising for extreme events may be through tabletop exercises. These can either be formal or informal evaluation or discussion-based exercises performed by key personnel. Tabletops are beneficial because they can involve leadership, players and observers from an unlimited number of entities who can be presented with comprehensive understanding of the disaster and affected area. Additionally, tabletops show value because they provide opportunity for representatives and technical specialists to collaborate and refine operational plans and policies. Moreover, tabletop exercises offer opportunities for people to identify the necessary points of contact for different agencies and business units.

Success is achieved when participants effectively identify and resolve issues in the overall process of response. Exercising for extreme events is likely to incorporate a multi-agency response. It is best for each entity to understand how their procedures and processes evolve when additional resources have become available, and when changes in command and control staff are expected. For example, a comprehensive training program in exercise design can be found through Homeland Security Exercise and Evaluation Program (HSEEP).

**The Extreme Event Scenario**

A well-developed scenario for extreme events should challenge the emergency management capability of an entire entity. Historically, extreme events have presented employees, management, and responders with an excruciating operational tempo during response and recovery phases. Replicating this tempo in an exercise can be extremely difficult; exercise officials (i.e. planners and controllers), must ensure the exercise injects occur quickly. Exercises based on acts of terrorism, electro-magnetic pulse, chemical, biological, radiological and nuclear event or severe weather are all viable options capable of being referenced through scientific data and historical facts. Entities can reference characteristics of such events to further scenarios and determine program effectiveness.

**Evaluation**

As described, exercises are used to evaluate a process in real time. The evaluation criteria must extend from the exercise objectives. Evaluations from FE’s and FSE’s rely on player integrity and knowledge that actions are to be carried out and reviewed for fluidity and effectiveness. Also discussed previously, in an extreme event, the entity will aggregate with other groups for a coordinated response. Entities are encouraged to establish memorandums of agreement (MOA)/ memorandums of understanding (MOU) with neighboring organizations to identify resources capable of being committed to an extreme event. The language in the MOU/MOA should not simply define the resource commitment, organizational alignment, and jurisdictional authority, but also highlight standards for performance by each organization.

**Engagement**

Finally, the most important element of an exercise is solicitation. Public and private entities from adjacent sectors may find the level of complexity of the electric grid to be intimidating. Utilities must push to break this barrier and include sectors to join and understand the impact an extreme event may have on the electric grid. A great place to start is with engaging local and state or provincial emergency management officials. Educating local and state or provincial EM officials and encouraging their participation will benefit their agencies by further promoting the stringent testing of their own capabilities.
Chapter 6: Resiliency

This section discusses resiliency as it applies to how effective entities can navigate through extreme events. In layman’s terms, resiliency describes toughness, or the ability to quickly rebound from situational setbacks. The reliability of the electric grid is contingent upon an entity’s resilience. Resilient entities are interdependent; they form a network in which each entity supports the grid; while mutually reliant, they each support and maintain their own assets. Like other networks, the grid is only as strong as its weakest point; a single entity that does not cultivate its own resilience in preparation for extreme events may potentially compromise the security of entire network.

The objective of resiliency is to minimize the time an entity is non-operational and increase the speed at which the entity can recover to full capacity and rejoin efforts to restore the grid. Three dimensions of resiliency will be discussed here. The first, structure resilience, refers to facilities or housing that protect personnel and systems from the elements. The second dimension, is the resiliency of people or employees who are prepared and capable of maintaining composure and rational thought through an extreme event while performing their duties. The third dimension, systems resilience, consists of a set of principles or procedures according to which something is done. In this context, systems also refer to mechanical or digital devices intended to enhance operability, such as cameras or industrial control devices.

Structural resiliency is to strengthen or reinforce the protective integrity of an enclosure to enhance its capability absorb damage caused by extreme events. Resilience is achieved by adapting enhancements through materials such as steel plating, or by engineering specifications designed to withstand force. Additionally, resiliency can be enhanced by the implementation of physical security features to the external surface of the structure. Designs such as window films that enhance the integrity of the glass, or barriers that can withstand the effects of blasting, cutting, or ramming on fences, walls or blocks, all contribute to the resiliency of a structure. Alternatively, resilience can also be achieved through the ability to rapidly repair assets and restore service. For example, it may make more sense to develop rapid repair capabilities for the restoration of transmission services rather than undertake expensive hardening of transmission towers.

The second dimension is ensuring resiliency through the workforce. This is the most complex, as it requires interaction amongst the multiple personality types that populate the entity. The pathway to personal resiliency is achieved and maintained by creating a culture geared towards personal development, adaptability, communication and teamwork. People are inherently resilient; good management fosters their resiliency by providing them with training and exercises that cultivate critical thinking. Conditioning employees to withstand stress in their individual roles strengthens the integrity of the team.

The third dimension is the resiliency of systems. This applies to both analog and digital systems that enhance an entity’s operability, and to the reinforcement of internal controls to prevent mis-operation and errors. Like facilities and employees, systems require rigorous testing, and continuous improvement to ensure sustainable operations through extreme events. Informed entities recognize that attacks on the grid are intended to disable and destroy. Thus, resilient entities must develop and train on robust processes to ensure stringent adherence to procedures that minimize failures and maximize that capacity to rapidly replace or recover those systems lost in the shortest amount of time.
An overarching principle for the developing of resiliency in structures, organizations, and systems is the application of redundancy. Redundancy is the basic principle applied to create continuity within the system to ensure no single point of failure exist. Principles of redundancy applied to communication systems, subject matter experts, or life support systems such as backup generators are beneficial during extreme events. Redundant systems present options to the strategic decision making of Incident Commanders, sustains quality of life for response and recovery teams, and ensures continuity of operations for management and stakeholders.

In conclusion, achieving resiliency requires effective interrelationship between structures, people and systems as described above. Entities must continually and comprehensively develop and maintain the resiliency of their personnel, systems and facilities. While there is no perfect strategy by which every entity can defend its assets, there will always be opportunities to adapt best practices to strengthen entity resilience. Applying the strategies of redundancy, continuous improvement, and adaptation to daily problems and emerging challenges are the ingredients for achieving resilience the face of extreme events.
Chapter 7: Information Sharing during Extreme Events

Protecting something as intricate as the electrical grid, requires a network of communication and information sharing. Retired General Stanley A. McChrystal once stated, “It takes a network to defend a network”. Extreme events present exceptional challenges to the capabilities of an entity’s decision-making cycle. To counteract extreme events, an entity depends upon a fundamental knowledge to understand data as it applies to extreme events. The speed at which information must be transmitted is a pivotal factor; facilitating, enabling or hindering leadership’s ability to think and react critically and effectively. The collaborative efforts of numerous entities can enhance the responsiveness of each to extreme events.

The Fundamentals
Entities should understand the foundation of an information sharing program is the accumulation of data. During extreme events, the application of data may allow entities to detect and resolve problems before they evolve into crisis, to evaluate the effectiveness of response, and to identify relationships between variables. Most importantly, the value of data during extreme events, 1.) allows management to think critically, 2.) provides responding personnel and organizations relevant information and tools, 3.) helps to enhance understanding of the operational environment, and 4.) facilitates informed decisions that lead to effective response and recovery operations. While data application plays large role in emergency preparedness and management operations, it has its limits. Because extreme events are statistical anomalies we cannot rely on data collected to fully predict extreme events. For example, man-made disasters (e.g. Deepwater Horizon, Three Mile Island) occur unexpectedly, typically due to mistakes or unforeseen failures in systems with little warning. The Root Cause Analysis on these events highlighted these disasters could have been avoided had system and human performance issues been detected early on. Criminal induced disasters like terrorism are typically carried out strategically and often under a high level of secrecy. Such events can be forecast with low certainty based on the data from historical trends and behavioral indicators; however, this data cannot definitively predict (e.g. dates, times, locations, etc.) such extreme events as terrorism. The sheer volume of data can be overwhelming and hinder useful application. Data that is well organized and well analyzed becomes information vital for effective prevention and response functions to extreme events. This information is essential to incident commanders, allowing them to determine relevance and provides a common operating picture. Incident response teams rely on the work of dedicated analysis to analyze collected information and to perpetuate the flow of information internally. The added value of continually updated information is that it reduces risk to responders during extreme events.

The Need for Speed
Effectiveness of the response during extreme events is heavily dependent on the speed at which information is delivered. The unprecedented pace at which an extreme event may unfold might exceed the capabilities of the entity. Thus, the timing at which informational products are released may only provide a snapshot of a given set of circumstances. Analysts who are experts in the subject matter may be able to formulate possible outcomes based on potential variables. At a bare minimum, information should be shared with incident commanders and others, allowing them to mitigate risk in their overall response strategy and build continuity among responders. As extreme events become increasing complex, so does the need for a more comprehensive approach to information exchanging. The potential for secondary or simultaneous attacks occurring against the Electrical Grid reinforces the need for expedited information exchange between entities. In a 2016 document drafted by the Physical Security Advisory Group “Electricity Sector and the Design Basis Threat” an attack on the grid will be the actions of dedicated, skilled, and coordinated actors, using multiple attack vectors such as physical, cyber and possibly unmanned Ariel
vehicles. Arguably, there is no absolute way to prevent future attacks, since a trained adversary will likely use speed, surprise and violence of action to their advantage. The best strategy is to strengthen the interdependence between entities as described and reinforce the speed and accuracy of information exchanged.

The nature of extreme events is to be fast-paced, possibly widespread, and to present dynamic risk factors. Thus, it is desirable when the flow of information is streamlined to approximate the speed at which the extreme event unfolds. Some best practices are implementing internal controls during extreme events to minimize or prioritize their information sources. This helps ensure that incident commanders are only receiving vetted, and pertinent information. This necessitates that entities design incident response programs that incorporate information channels to control flow of information during extreme events. Recent revisions to the FEMA Incident Command System now include an Intelligence & Investigation Section, reporting directly to the Incident Commander.

**The Network**

Sources of data applicable to extreme events are likely to originate from inter-entity condition reporting, cross-industry information sharing networks, Human Intelligence (HUMINT) and Open Source intelligence (OSINT). More specifically, HUMINT relies on the vigilance of employees, community members and law enforcement officers to detect and report activity, making it relevant for emergencies. The effectiveness of HUMINT may be limited by human performance; the chaos of disasters may result in subtle details going unnoticed, thus stifling the ability to obtain clear data. OSINT, such as databases, intelligence products from credible sources, and social media, adds to the collection of raw data and perhaps validates HUMINT contributions to the Common Operating Picture (COP)². Additionally, social media serves best in extreme events when it effectively details the parameters of the event, thus filling a need for information-sharing network enhancements, and rapid information exchange.

The information sharing network should always begin within an entity. Employees should be encouraged to identify problems at any moment. During extreme events, employees may become key role players, supporting response and recovery operations. Fostering employee vigilance and promoting prompt reporting behaviors will strengthen response by mitigating risk. Adopting the DHS “See Something Say Something” practice it is an effective starting point, particularly when entities tailor this program to their specific capabilities.

The expansion of the information sharing network should begin with business units. The strength of the network is reliant on each business units’ ability to collaborate with external peer business units from local entities and intelligence organizations. Although not a requirement, entities should make every effort to become a part of such networks, participating in information exchange helps to paint a picture of the threat landscape. An advantage of this network is preparation for extreme events, as neighboring entities can provide peer evaluations and contribute to effective assessment of risk and vulnerability. When extreme events are imminent, neighboring entities may offer mutual assistance as well as pass along information, thus also contributing to the COP.

Entities involved in extreme physical security events are likely to engage the local, state and federal law enforcement agencies, including the local officials from the FBI and the Royal Canadian Mounted Police. These agencies respond and contribute to the flow of information via investigations and criminal intelligence. Currently, local and state enforcement agencies, are expanding their information distribution into critical infrastructure and key resources. They provide utilities additional information to further identify and mitigate threats.

---

² Common Operating Picture (COP) - Single identical display of relevant operational information (i.e. locations of responders, status of resources, scene details) shared by more than one command element.
Finally, the Electricity Information Sharing and Analysis Center (EISAC) is an information sharing entity exclusive to the electric utility industry. It ensures the delivery of physical and cyber security threat intelligence to owners and operators. The benefits of the EISAC is to capture threat information from various sources and to distribute information throughout the industry. Applied to extreme events, the EISAC adds value by obtaining details of events and continually updating owners and operators, thus further enhancing vigilance throughout the industry in preparation for subsequent hostile actions.

Historically, the need to gather and share information has been viewed as the primary role of our nation’s security apparatus. We must not forget who owns and operates the system that ensures the delivery of reliable electricity throughout the nation, ensuring its survivability. We, too, are responsible for upholding national security. Extreme events induced by acts of terrorism can succeed only if the industry fails to collaborate in creating a network so great and so effective that adversarial efforts will fail, even on our worst day.
Chapter 8: Definitions

**Extreme Events** – An event that has the potential to damage or severely impair an organization’s ability to operate.

**Physical Security Assessment** – The evaluation of physical access controls for a facility.

**Resilience** is defined as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Examples of resilience measures:
- Developing a business continuity plan
- Having a generator for back-up power
- Using building materials that are more durable

**Vulnerability Assessment** – Evaluating the possibility of a facility being attacked.

Related Documents and Links

- Security Guideline for the Electricity Sector: Physical Security

---

1 FEMA Course E/L0104 Introduction to exercise Design
## Revision History

<table>
<thead>
<tr>
<th>Draft Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Version 1</td>
<td>August 2, 2017</td>
</tr>
<tr>
<td>Draft Version 2</td>
<td>August 11, 2017</td>
</tr>
<tr>
<td>Draft Version 3</td>
<td>August 16, 2017</td>
</tr>
<tr>
<td>Draft Version 3.8</td>
<td>December 4, 2017</td>
</tr>
<tr>
<td>Draft Version 4.1</td>
<td>December 20, 2017</td>
</tr>
<tr>
<td>Draft Version 4.2</td>
<td>March 5, 2018</td>
</tr>
</tbody>
</table>