IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

RESILIENT POWER BEST PRACTICES

OVERVIEW

The Resilient Power Best Practices fact sheet summarizes best practice recommendations from the Cybersecurity and Infrastructure Security Agency (CISA)-led Resilient Power Working Group, consisting of members across the federal government, state and local governments, non-profits, and private industry. These critical communications infrastructure best practices should be a part of comprehensive, risk-informed Business Continuity and Continuity of Operations (COOP) plans, developed per the *Federal Emergency Management Agency (FEMA) guidance*.

For many sites, implementing these resiliency best practices is inexpensive and may reduce the total cost of ownership.

BACKGROUND

Natural events, such as earthquakes, hurricanes, fires, floods, winter weather and solar storms, and manmade threats such as physical attacks, cyberattacks, and electromagnetic (EM) attacks pose risks to the grid that could have cascading effects and leave critical facilities reliant on their own power generation and energy storage capabilities for an extended period of time. The best practices discussed here were developed to help executives, chief engineers, emergency preparedness and continuity planning personnel, cyber and physical security engineers, and telecommunications and information technology (IT) staff maintain power to critical communications and associated equipment at key facilities under all hazards to preserve life, health, and societal well-being.

SCOPE

The *Resilient Power Best Practices* document, expected to be released around the third quarter of 2021, furnishes comprehensive guidance to address the following topics:

- Power resilience levels for critical communications infrastructure related facilities and sites
- Emergency and backup power generation systems
- Facility/site operations and maintenance
- Power transfer systems, energy storage, and microgrids
- Cybersecurity, physical security, and EM security

The scope does not include best practices for electrical or natural gas utilities, or federal response efforts.

POWER RESILIENCE LEVELS

To easily identify the resilient power best practices that the communications infrastructure owners/operators may want to use for planning, procurement, and implementation purposes, four resilience levels are defined:

These resilience levels can help organizations implement their requirements and should not supersede them.

- **Level 1 Resilience** – Least-cost best practices that provide a commercially reasonable chance of maintaining power for at least **three days under *all-hazards*** (for example, three days of fuel is stored onsite to maintain critical loads).
- **Level 2 Resilience** – Provides a best-efforts approach to maintain power for at least **seven days under *all-hazards***.
- **Level 3 Resilience** – Generally covers the most critical infrastructure where power should be sustained **under *all-hazards* for a minimum of 30 days**.
- **Level 4 Resilience** – Typically limited to the most critical military/federal/National Essential Functions communications infrastructure where **power should be sustained with no unplanned downtime under *all-hazards* in excess of 30 days**.

BEST PRACTICES

Additional background material, analysis, guidelines, and references are provided in the *Resilient Power Best Practices* document to identify and implement the processes and solutions for each facility/site.

Function	Design and Process Best Practices High-Level Summary
Backup Generation Sources	• Maintain at least two backup generation sources for Level 2 Resilience and higher. • Ensure the backup generation sources achieve the longevity per the desired resilience level. • Perform regularly scheduled maintenance and load testing. • Consider fuel diversification to prevent fuel supply disruptions.
Fuel	• Store enough fuel onsite to meet the desired "all hazards" resiliency level. • Deploy a fuel maintenance process, including fuel rotation. • Regularly assess fuel delivery contracts and understand potential emergency delivery alternatives.
Load Segmentation and Microgrids	• Segment power loads to conserve resources so that mission-critical loads are adequately powered. • Consider implementing an all-hazards secure microgrid in Level 3 and 4 sites or on large campuses.
ATS and Control System	• Install electromagnetic pulse (EMP) hardened automatic transfer switch (ATS) solutions to protect important assets by automatically disconnecting them from the commercial power grid. • Maintain protected, redundant industrial control systems.
Energy Storage and Renewable Energy	• Deploy uninterruptible power supply (UPS) systems to support sensitive critical systems. • Consider implementing a renewable energy hybrid system (REHS), which combines renewables with a battery energy storage system (BESS) and a 24/7 backup generation system, to extend fuel supplies and improve power resilience while saving electricity costs (on an annual basis).
Tele-communications	• Ensure mission critical telecommunications are prioritized for emergency power and integrated in the Operations and Maintenance Plan (O&M). • Deploy telecommunications diversity (e.g., cellular, satellite, landline, high frequency [HF] radio) and follow the PACE model (Primary, Alternate, Contingency, and Emergency) if immediate communications are needed.
Process, Governance and Maintenance	• Conduct regular audits to ensure that the O&M Plan's Planning, Organization, Equipment, Training, and Exercises (POETE) supports the desired resilience level. • Include preparedness of employees and vital external businesses in the O&M Plan to ensure continuity of operations during extreme events. • Establish processes to "stress test" readiness through periodic plan reviews, operational tests, and table-top and "real world" exercises.
Cybersecurity	• Follow industry cybersecurity standards, e.g., NERC CIP-009-6, NIST Cybersecurity Framework. • Include supply chain security in the cybersecurity plan.
Physical Security	• Add specific threats, existing security, and site vulnerabilities into the physical security plan. • Red team the physical security plan by working with local law enforcement & security contractors.
Electromagnetic (EM) Security	• Implement protections against the effects of EM events, including lightning, High-altitude EMP (HEMP) (particularly the higher frequency E1 HEMP), and Intentional EM Interference (IEMI).

This fact sheet may be downloaded from cisa.gov/shared-resources-shares-high-frequency-hf-radio-program. For more information or to seek additional help, please contact Resilient.Power@cisa.dhs.gov.