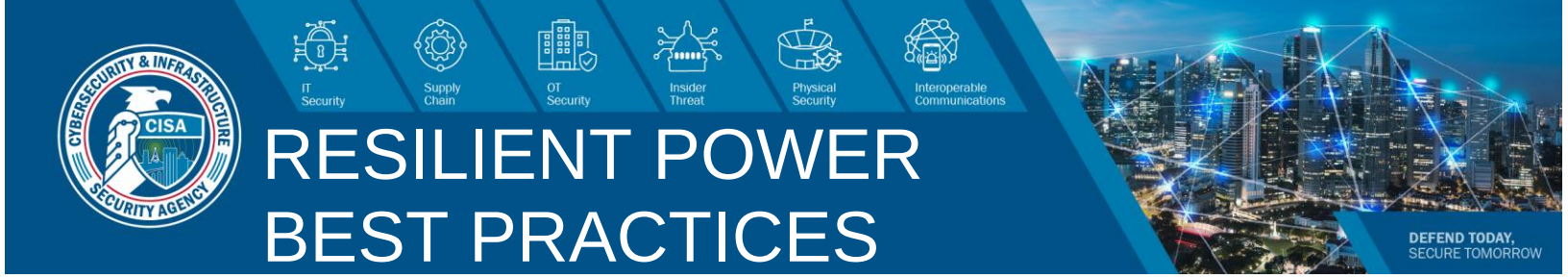

RESILIENT POWER BEST PRACTICES

OVERVIEW

The *Resilient Power Best Practices for Critical Facilities and Sites* fact sheet summarizes the 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 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 cyberattacks, physical attacks, 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 infrastructure at key facilities based upon the organization's risk management plan to preserve life, health, and societal well-being.

SCOPE

The *Resilient Power Best Practices* document furnishes comprehensive guidance to address the following topics:

- Power resilience levels for critical 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 infrastructure owners/operators may want to use for planning, procurement, and implementation purposes, four resilience levels are defined. The organizational requirements and the local conditions including the time required for power to be restored and for fuel to be delivered under the identified risk factors may lead to more or less time than suggested below for backup power to be maintained.

- **Level 1 Resilience** – Incorporates cost effective best practices to maintain power to critical operations. Typically, expendable supplies, such as fuel, should be maintained for three days under "all hazards."
- **Level 2 Resilience** – Extends Level 1's cost-effective practices to further improve power resiliency. Typically, expendable supplies, such as fuel, should be maintained for seven days under "all hazards."
- **Level 3 Resilience** – Implements additional measures beyond Level 2 to further improve power resiliency. Typically, expendable supplies, such as fuel, should be maintained for around 30 days under "all hazards."
- **Level 4 Resilience** – Power should be sustained with no unplanned downtime. Typically this is limited to the most critical military/federal/National Essential Functions.

BEST PRACTICES

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

Functional Area	Design and Process Best Practice Highlights
Process, Governance and Maintenance	• Document a risk management plan that includes the resilient power threat environment, the vulnerabilities, and the organizational risk tolerance associated with the identified risks. • Determine resiliency level needed, document requirements, and conduct gap analysis. • Join appropriate sector/geographically based information sharing organizations such as InfraGard, the National Council of ISACs and preparedness networks like your local CERT. • Schedule regular audits to ensure that the Planning, Organization, Equipment, Training, and Exercises in the Operation and Maintenance Plan 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.
Backup Generation Sources	• Maintain at least two backup generation sources for Level 3 Resilience and typically for Level 2 unless the primary and backup power sources are resilient enough to meet Level 2. • Level 4 sites should utilize two independent utility/primary power sources plus two independent and geographically separated (within the site) backup power sources. • Ensure the backup generation sources achieve longevity per the desired resilience level. • Perform and document 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 document emergency delivery alternatives.
Control Systems and Microgrids	• Segment power loads and conserve resources so that critical loads are adequately powered. • Consider implementing an all-hazards secure microgrid in Level 3 sites or on large campuses. • Maintain protected, redundant industrial control systems and electrical distribution systems.
Renewable Energy and Energy Storage	• Consider implementing a renewable energy hybrid system (REHS), which combines renewables with an energy storage system (ESS) and a 24/7 backup generation system, to extend fuel supplies and improve power resilience while reducing annual electricity costs. • Deploy uninterruptible power supply (UPS) systems to support sensitive critical systems.
Tele-communications	• Ensure mission-critical telecommunications are prioritized for emergency power and integrated into the Operations and Maintenance Plan. • 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.
Cybersecurity	• Include supply chain security and a zero-trust security model in the cybersecurity plan. • Follow industry cybersecurity standards, e.g., NERC CIP-009-6, NIST Cybersecurity Framework.
Physical Security	• Add specific threats, existing security, and site vulnerabilities into the physical security plan. • Red team the physical security plan by working with law enforcement and security contractors.
Electromagnetic (EM) Security	• Implement mitigations to help protect against the EM effects of lightning, E1 High-altitude EM Pulse (HEMP), E3 HEMP and Geomagnetic Disturbance (GMD) (as needed), and Intentional EM Interference (IEMI).

This fact sheet may be downloaded from https://www.cisa.gov/resilient-power-working-group.