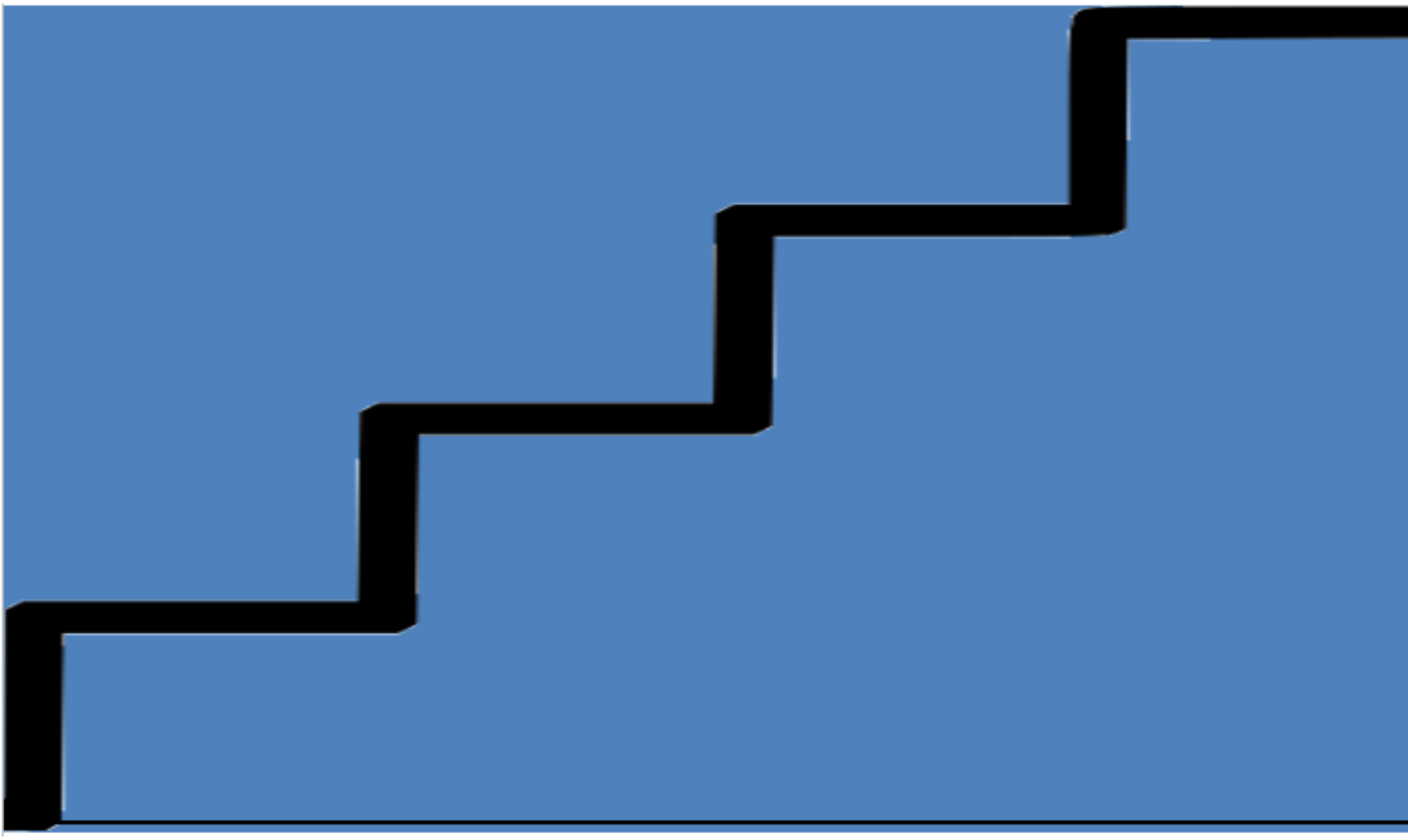


Ten Steps of Resilient Power

For Critical Infrastructure Facilities and Sites to Ensure Continuity of Business and Operations

August 2024

Cybersecurity and Infrastructure Security Agency (CISA)
Resilient Power Working Group (RPWG)

EXECUTIVE SUMMARY

These *Ten Steps of Resilient Power* ("*Ten Steps*") consist of process-oriented guidelines to help best implement the *CISA Resilient Power Best Practices for Critical Facilities and Sites*[1] ("*RPBP*") using the *CISA Resilient Power Assessment Worksheet*.[2] The RPBP provides extensive best practices and includes the rationale and various considerations for the guidelines to help protect against short- and long-term power outages.

These Ten Steps and the RPBP can help critical infrastructure organizations (excluding electric and natural gas utilities) implement a comprehensive, risk-informed Business Continuity and Continuity of Operations (COOP) resilient power plan. Prior to starting the first step, designate a project champion who should then identify a lead, as shown in Figure 1 below.

Ten Steps of Resilient Power

1. Identify Lead and Establish Team
2. Write Project Charter
3. Document Requirements
4. Conduct Assessment and Perform Gap Analysis
5. Create Project Management Plan
6. Research Backup Power Solutions
7. Determine Security Mitigations
8. Develop Implementation Plan
9. Update Operations and Maintenance (O&M) Plan
10. Implement Power and O&M Plans

Figure 1. Ten Steps to Implement Resilient Power

The Ten Steps are flexible and should be tailored to the specific organization often by implementing the highest value improvements first including properly maintaining the fuel and the backup power generation system. These Ten Steps were developed based upon the *RPBP, Federal Emergency Management Agency (FEMA) guidance*[3], and industry best practices (e.g., *Program Management Institute's Project Management Body of Knowledge*[4]*).*

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity and Infrastructure Security Agency (CISA) resilient power companion documents:

- *Resilient Power Best Practices for Critical Facilities and Sites*[5] ("RPBP")
- *Resilient Power Working Group | CISA*[6] ("RPWG")
- Use either one of the above links for the following documents:
- Resilient Power Best Practices Fact Sheet ("RPBP Fact Sheet")
- Resilient Power Assessment Worksheet

The *Ten Steps of Resilient Power* ("*Ten Steps*") recommend potential actions to implement the CISA *RPBP*. The *RPBP* discusses best practices to help prevent short- and long-term outages to critical facilities and sites (excluding electric natural gas utilities).

These *Ten Steps* recognize that there are trade-offs that often must be made between resilience and budget. The best resilient power solution depends upon (i) the requirements, (ii) the gap between the requirements and the existing solution, and (iii) the budget. Consider a spiral or iterative model to first implement the simplest, highest value solutions that are within the allocated budget. Subsequently, the longer lead time or more costly solutions could be implemented perhaps after obtaining the necessary budget. All best practices should be a part of a comprehensive, risk-informed Business Continuity and Continuity of Operations (COOP) plan developed per *Federal Emergency Management Agency (FEMA) guidance*[7].

These Ten Steps should be performed periodically or when it is believed that the facility's or site's resilient power system requires major changes to meet the organization's COOP plan. If this is a periodic review of the existing requirements and system, some steps such as the charter in Step 2 may not be required unless substantial changes are needed.

The first step starts with the critical infrastructure organization assigning a resilient power champion. This champion, typically with budget authority, should become familiar with each step in this document, in the *CISA Resilient Power Assessment Worksheet* and in the *RPBP*. The champion should then identify a project leader as shown in Figure 2 below. The specific steps below may be performed in a different order than shown. For instance, the organization may conduct an assessment and then write a charter after determining that an extensive amount of work is required.

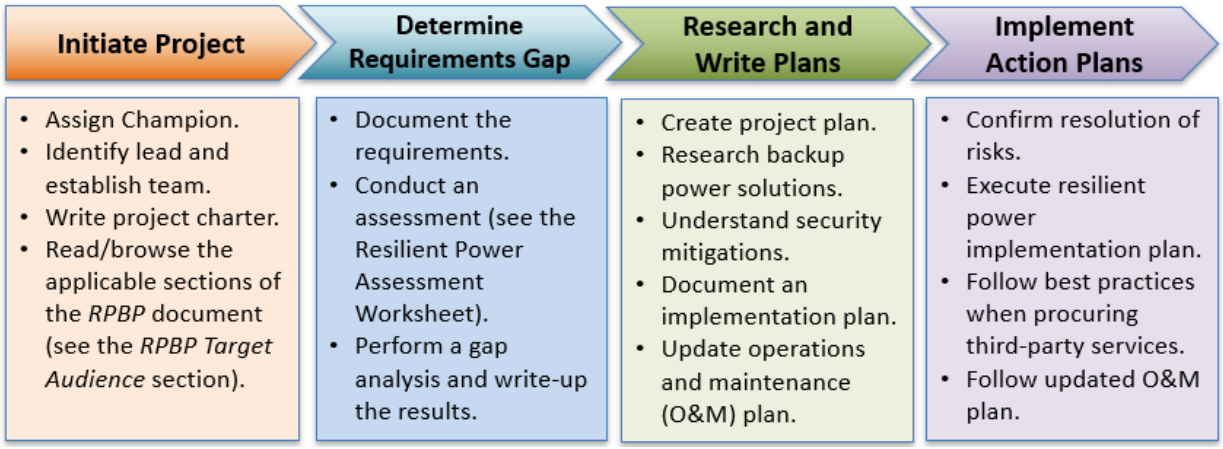


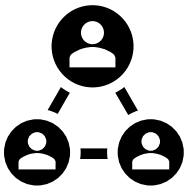
Figure 2. The Four Resilient Power Phases

The *RPBP* and these *Ten Steps* were developed by CISA's RPWG. The RPWG comprises of representatives from various federal, state, and local government departments and agencies, non-governmental organizations, and private industry. This document assumes that the organization is evaluating its entire backup power system and not just planning to make small changes (e.g., updating the generator maintenance procedure).

1 IDENTIFY LEAD AND ESTABLISH TEAM

Project Champion and Lead Preparation:

- Read RPBP Target Audience / How to Use This Document.
- Read RPBP Executive Summary, Chapter 1 (*Introduction*), and Chapter 2 (*Best Practices*).
- Read/browse the applicable sections after *RPBP* Chapter 2.
- Read the facility's/site's risk management plan.

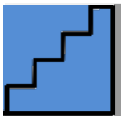


The first step after obtaining a project champion is to identify a **project lead** as discussed in CISA's "*Infrastructure Resilience Planning Framework (IRPF)*[8].The lead will usually report to the project champion or sometimes will be the project champion. The project lead should understand the facility's/site's resilient power system and key risks, engage stakeholders, and perform administrative, coordination, and event-planning functions.

The project lead and the project champion should establish the diverse team needed for this endeavor. The positions mentioned in the *RPBP* Target Audience section, including the employees, contractors, and third parties in the following categories should be part of that *Resilient Power Team* depending upon the overall project goals and objectives:

- Power engineering and management

- Continuity planning, government, and business emergency preparedness
- Operations and maintenance
- Procurement and those involved in the acquisitions of power-related systems or components (e.g., finance)
- Security: cybersecurity, physical security, and facilities
- Telecommunications, electromagnetic (EM) security, and information technology (IT).



2 WRITE PROJECT CHARTER

Resilient Power Team Preparation:

- Read the material in Step 1 that is applicable to your role in the project including reading the introductory material in the *RPBP*.

Once a project lead is assigned and the team is established, the second step is for the project lead to work with the project champion to write a resilient power project charter. Per the Department of Health and Human Services (HHS) a "Project Charter formally authorizes the existence of a project and provides the Project Manager (PM) with the authority to proceed and apply organizational resources to the project. The Project Charter will reflect the goals and objectives of the project at a specific point in time and needs to be kept under configuration control and updated, as needed, to reflect changes to project scope, schedule, and/or cost."[9]

Prior to organizing the resilient power team, the project lead should write a project overview including its scope, list potential resources and reference existing high-level resilient power-related information. This material will enable the group members to quickly review relevant material to better understand the landscape before providing input.

Subsequently, the planning group can be created and complete the project charter, including adding the following information:

- Project overview (update the one that the project lead wrote)
- Measurable project objectives and related success criteria
- High-level requirements
- High-level project description
- High-level risks (reference the risk management plan)
- Summary milestone schedule
- Summary budget (consider splitting into "Committed Budget" and "Potential Budget")
- Team members.

For a sample template, see "*Project Charter Template | Texas Department of Information Resources*."[10]

Both because the project likely hasn't been fully defined at this point and many critical infrastructure resilience projects are dependent upon outside or atypical funding sources, some of the above might be divided into approved and funded project tasks versus potential work. The above objectives and requirements, based upon the organization's risk management plan, should include the below resilient power information as well as other mission critical requirements:

- The mission critical objectives.
- The resilience required, including the minimum number of days the critical infrastructure needs to operate during an outage and the downtime allowed (if any). One or a combination of the four resilience levels shown below and defined in the *RPBP* could be used to help describe these high-level resilience requirements (see the *Definition of Resilience Levels* section in the *RPBP Introduction* for details).

RPBP Four Levels of Resilience

Level 1: Cost effective implementation typically with three days of supplies (e.g., fuel).
Level 2: More advanced best practices typically with seven days of supplies.
Level 3: Resilience includes more redundancy and typically 30 days of supplies.
Level 4: No unplanned downtime limited to the most critical infrastructure (e.g., military).

Figure 3: Resilient Power Best Practices Four Levels of Resilience

- To help determine the resilience and reliability needed, calculate the Value of Lost Load (VoLL), which includes the estimated potential harm to your stakeholders as well as direct revenue loss. (For more details about VoLL, see the National Renewable Energy Laboratory (NREL) website or the RPBP *Renewable Energy Hybrid System (REHS) Sample Use Cases* section.)
- List the RPBP topic areas that will be covered, such as fuel storage, fuel delivery, generation sources, maintenance, cybersecurity, external dependencies, employee/contractor requirements, etc.
- The facility(s), site(s), and equipment that are being addressed.
- The rationale for the above.

Consider a consensus-based estimation technique such as Wideband Delphi to determine the schedule and budget. These prediction methods are particularly helpful in more complicated projects or if there is a diverse opinion regarding schedule or budget impacting issues since these techniques can be used to help understand other people's viewpoints more easily and quickly.

3 DOCUMENT REQUIREMENTS

Resilient Power Team Preparation:

- Review the RPBP's Chapter 2 Risk Management Plan and the Resilient Power Requirements.
- Read a best practices document such as Project Management Institute's (PMI's) Project Management Body of Knowledge (PMBOK) Project Risk Management section and PMI's requirements guidelines.
- Review the requirements from other facilities and sites with similar overall resilience objectives.

Key stakeholders should be identified for each requirement category.

To best understand the resilient power requirements of a critical infrastructure facility/site, it is critical to understand the mission as discussed in the RPBP. The risk management plan should be updated to account for risks that may negatively impact the facility's/site's power. The risk management plan should discuss the importance of the infrastructure sector and the role of that facility or site to help the enterprise meet its resilience goals and objectives within the sector. The facility's or site's mission and criticality will then drive the resilient power high-level requirements, and subsequently, the low-level requirements.

Some of the key drivers of these requirements should be:

- Your **risk management plan**, which is the primary driver of the requirements.
- **Minimize common mode failures** where there are failures across a sector, sites, or facilities due to a common problem or risks (see RPBP). Two examples of this include:
- Having issues with a single cellular site might not be critical but losing power to multiple sites in the same area could be critical, which is much more likely to occur when using the same design and equipment from site to site.
- Using two telecommunications services provides extra resilience but much of that extra resilience could be lost if both services use common telecommunication lines.
- **Process improvements** (e.g., how often fuel is tested) in addition to supplies and equipment purchase requirements.
- **Potential indirect power-related issues**, including contractors or employees who might not be able to drive to the facility/site if the outage was caused by extreme weather or an attack or perhaps the utility cannot provide clean water making the building uninhabitable, etc.
- **Typical and peak loads** (including equipment start-up) when occupied during a COOP event (versus normal state).

Prioritize the requirements and actions to reduce risk via an engineering-based risk reduction method such as Failure Modes and Effects Analysis (FMEA). For more details regarding how to use FMEA, see the Centers for Medicare and Medicaid Services (CMS) document *Guidance for Performing Failure Mode and Effects Analysis with Performance Improvement Projects*.

The high-level resilient power requirements will feed into the project's low-level requirements and specifications that can be used by procurement and the implementation team. For instance, a high-level requirement that the backup power system must be able to meet the critical equipment load demands for three days without additional fuel being delivered would help drive the size of the fuel storage container (e.g., a 4,500-gallon container would be needed for a system that is estimated to use 1,500 gallons/day during an outage).

Lastly, note the areas that are out scope for project implementation. For example, the cybersecurity team may request that they handle all cybersecurity requirements. However, the resilient power team should still work with the cybersecurity team and needs to be responsible for manual overrides where applicable (e.g., manually transferring power to a generator).

4 CONDUCT ASSESSMENT AND PERFORM GAP ANALYSIS

Resilient Power Team Preparation: Review the *CISA Resilient Power Assessment Worksheet*.

After documenting the requirements, the suggested next step is to conduct an assessment and then perform a gap analysis as shown in Figure 4 below. Use CISA's *Resilient Power Assessment Worksheet* to help conduct this assessment.

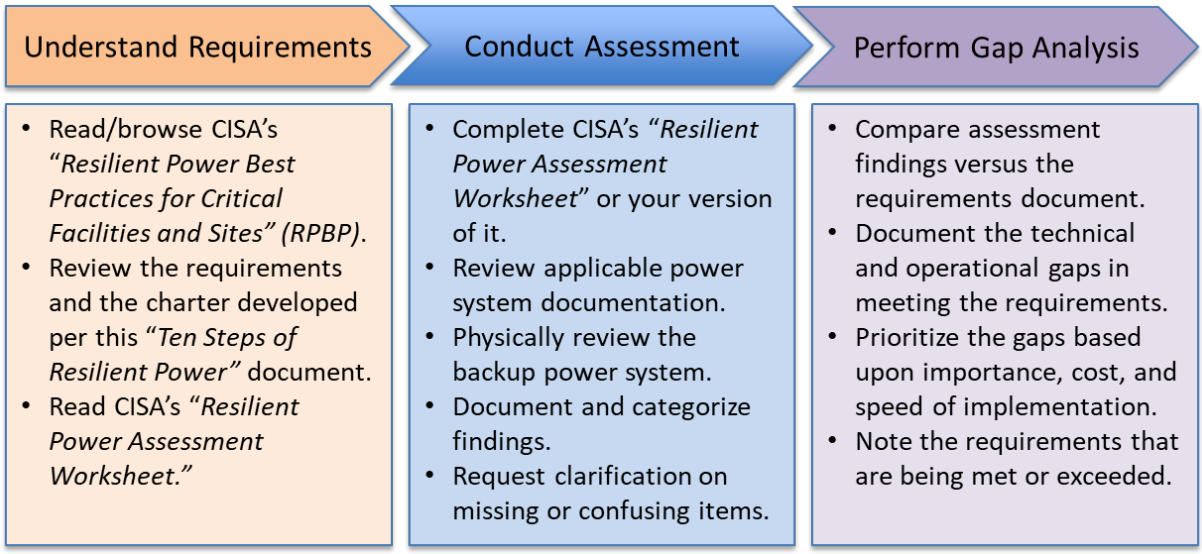


Figure 4. Conduct Assessment and Perform Gap Analysis

The gap analysis checks each requirement developed in the previous step against the existing resilient power solution and processes, including resources that might be available externally to the facility/site. Thus, if the requirement is to have a high likelihood of operating for three days during a grid power outage but if there is only enough fuel onsite for two days and there is no near-guaranteed fuel supply nearby, that could be a gap. Further, if the resilient power plan assumed that fuel could be delivered after two days from the start of the grid disruption, but the resilient power team does not see adequate evidence that fuel would be delivered in that timeframe under some of the scenarios listed in the organization's risk management plan, that too would be a gap.

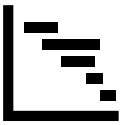
To conduct the assessment, follow CISA's *Resilient Power Assessment Worksheet*. This worksheet helps critical infrastructure owners and operators collect the necessary data to analyze their facility's or site's backup/emergency power solution and processes (e.g., testing) per their requirements.

Consider *CISA's Resilient Power Assessment Worksheet* to conduct the assessment and gap analysis.

Using the RPBP-defined resilience levels can make it easier to perform a self-assessment or for a third party to conduct an assessment. The gap analysis will feed into the remaining steps of this document.

5 CREATE PROJECT MANAGEMENT PLAN

Project Lead Preparation: Review a standardized project management plan (PMP) template.



Using the gap analysis completed in the previous step, create a PMP. Per the PMI *PMBOK® Guide Fourth Edition (Chapter 3),* the PMP is "the process of documenting the actions necessary to define, prepare, integrate, and coordinate all subsidiary plans." It describes "how the project will be planned, executed, monitored and controlled, and closed." Some of the major activities in the PMP are:

- Collect requirements.
- Write a detailed description of the project and products.
- Develop a schedule including creating a work breakdown structure.
- Estimate costs and develop a budget.
- Consider splitting into available budget and potential budget.
- Include funding from selling power into the grid if installing a primary generation source (e.g., Type 4 diesel generator, solar).
- See the PMBOK Guide for additional potential major activities (e.g., quality plan, risk management plan).

Even if the resilient power lead does not know what the final resilient power solution will be, a PMP should still be created and updated as needed. For instance, if the resilient power team wants to investigate a renewable solution but a cost/benefit analysis needs to be completed, the PMP could just include researching the renewable solution. Adding the implementation of that renewable solution to the PMP would only occur once the research is completed and funding is approved.

As discussed above, this PMP should be a living document particularly if much of the research still needs to be completed. The details of a PMP are extensively discussed in other documents, such as in PMI's PMBOK, so the PMP will not be discussed further in this step. After completing the PMP, the project lead and the project champion may want to update the resilient power project charter since it is now better known what needs to be accomplished.

6 RESEARCH RESILIENT POWER SOLUTIONS

Resilient Power Team Preparation:

- Each team member should read the sections in RPBP Chapters 5-9 that apply to their role in the project.
- Review the applicable resilient power solutions from best-in-class similar facilities and sites.

First, research the applicable resilient power technologies and vendors (security is discussed in Step 7). This research may include the following potential solutions within the RPBP depending upon the project scope:

- **Diesel generators** – Diesel is the core backup power generation energy solution for most facilities/sites. A Type 1 diesel generator is only expected to run up to 200 hours annually while a Type 4 can be run 24/7 for primary power generation and can be used to charge an energy storage system (see ESS bullet below).
- **Fuel** – Fuel maintenance is often the most overlooked part of a resilient power solution although fuel storage and fuel delivery are also critical. Maintenance includes testing of the fuel, enhancing the fuel quality, and ensuring that the right type of fuel is being used given the season.
- **Natural gas generators** – These are a cleaner backup power generation solution than diesel and do not have the fuel quality issues associated with diesel. However, pipeline delivery systems typically limit this solution being deployed at higher resilience sites as noted in the RPBP since long pipelines can be unreliable particularly during catastrophic events. Further, it is much more difficult to store large amounts of natural gas or propane than diesel although a dual-fuel natural gas/diesel generator can resolve this issue.
- **Energy storage systems (ESS)** – Uninterruptible power supply (UPS) systems are a key part of a resilient power solution for systems that cannot tolerate voltage spikes or short-term power outages while a generator is being started. For renewable systems where a battery system may be used daily, lithium-ion battery ESS (BESS) solutions have gained traction.
- **Control Systems** – As a minimum, power transfer systems should be researched. It is also recommended that load segmentation be implemented to save fuel primarily so that the critical infrastructure can operate for a longer period of time using less fuel.
- **Microgrids** -- These are recommended when used with renewables but can also apply to traditional power generation systems particularly if using an Environmental Protection Agency (EPA) approved generator that can be operated for primary power.
- **Solar power** – The RPBP recommends using solar as a hybrid backup power solution together with a diesel or natural gas generator. Solar panels are inexpensive relative to the cost of an overall backup power solution, but the energy source is intermittent and there are other costs that need to be considered.
- **Other power generation sources** – Fuel cells, geothermal, and small hydroelectric power plants could be beneficial in some situations and small modular reactors (SMRs) have tremendous potential in the future as discussed in the *RPBP*.

The resilient power team should generally review new technologies as well as traditional ones as discussed above. For instance, the RPBP shows an example of solar power combined with a generator and a BESS to create a renewable energy hybrid system (REHS) to provide significantly improved resilient power versus just using a generator.

The team should also research which proposed solution(s) may be helped or hindered by the local environment, regulations, grant programs, and community power generation preferences or aversions.

7 DETERMINE SECURITY MITIGATIONS

Resilient Power Team Preparation: – Read/browse the following *RPBP* chapters:

- Chapter 3 Cybersecurity and Physical Security
- Chapter 4 Electromagnetic (EM) Security

Research applicable cybersecurity, physical security, and EM security solutions either after Step 6 or in parallel with it. The basic mitigation approach to each of these security areas is briefly described below. The resilient power team should view the mitigations holistically since there can be many interactions between each security category. For instance, securing a room often involves both physical security (e.g., a locked door) and cybersecurity (for verification purposes). Further, EM security might be involved as well if the verification or alert system could be disrupted through an EM event.

For cybersecurity, the RPBP recommends that the power system be included in the overall cybersecurity plan. Assuming zero trust security is implemented, which is a CISA recommended best practice, the industrial control system (ICS) cybersecurity plan can be merged with the IT cybersecurity plan (since there is zero trust even within a network). The cybersecurity plans should include adding ICS network-based cybersecurity requirements discussed in the *RPBP*, such as implementing geofencing to access the ICS network.

Supply chain requirements are another potential issue. A vendor can be a systemic, widespread problem if many critical infrastructure providers rely upon the same vendor or rely upon vendors from the same potentially hostile country or block of hostile countries.

Likewise, the resilient power components should be part of the physical security plan. Potential backup power issues include downed power cables and stolen fuel. The fuel issue can be a particularly major problem when a devastating power outage results in fuel supplies being disrupted.

Lastly, consider the EM security measures recommended in the *RPBP*. Most of the recommendations for Level 1-3 facilities are inexpensive or can even be implemented at no extra cost particularly if designed for new construction or equipment buildouts. For instance, the cost of an EM Pulse (EMP)-rated surge protection device (SPD) versus a more commonly deployed SPD is typically nominal compared to the overall cost of a new installation and the lifecycle costs may even be similar when accounting for the long life of an EMP-rated SPD. Other recommendations such as ensuring good bonding and good grounding are best practices regardless of the probability of an EMP event.

8 DEVELOP IMPLEMENTATION PLAN

Resilient Power Team Preparation – All applicable *RPBP* sections should have been read or browsed.

After documenting the requirements, the existing power system, and the potential solutions, the resilient power team should create a resilient power implementation plan. The implementation plan should prioritize the potential projects and tasks to optimally lower risk in a timely manner within budgetary and resource constraints. For instance, performing fuel tests more often is inexpensive and very quick to implement. Thus, increased fuel testing will typically improve resilience more quickly than buying a second generator. If grants or additional budget could become available, identify the items that will be implemented with the additional funding.

The implementation plan should translate the high-level requirements and the gap analysis into lower-level project requirements that can be used by the implementation team including the procurement team. For instance, in Step *3 DOCUMENT RISKS AND REQUIREMENTS,* if it specified that the critical systems and equipment must operate properly for at least three (3) days, this might translate into purchasing a 4,500-gallon (or 5,000-gallon) fuel storage container assuming that the backup power generation system may use 1,500 gallons per day during an outage.

Some of the potential sections of this resilient power plan could include the following:

- Core Backup Generation Source(s) – Discuss the type and size of any core power generation source(s) that will be purchased and any generators that may be available for emergency situations (e.g., the county's emergency management office may have temporary emergency generators available). Include the protocols for requesting a temporary generator and the facility-site associated logistics, such as the resources needed to connect a temporary generator which the generator supplier may not be provide, e.g., cabling, qualified installation personnel.
- Renewable Energy Generation Source(s) – Describe the type of renewable energy, the space required, the components needed, the maximum and expected generation capacity, and how the renewable energy generation system will improve the overall resilient power plan. Note that on occasion, this could be the core backup generation source (e.g., with a fuel cell).
- Fuel– Specify the fuel storage container's general size, type, and location and any fuel that is available from nearby sources that could replace or augment the fuel stored onsite. Include a discussion of how much fuel is expected to be used under various threat scenarios, the estimated fuel that will be available (is the fuel container always full or close to full?), and how long the fuel will last under the identified threat scenarios.
- Energy Storage – Cover the UPS system required for sensitive electronics and the BESS if applicable.
- Power Transfer System and Microgrid – Discuss the control system of the various power generation sources (e.g., automatic transfer switch (ATS)) and the control of the loads including any load prioritization. If implementing a microgrid, delineate any plans to sell electricity into the grid.
- Cybersecurity – The power system's ICS cybersecurity plan should be part of the facility's cybersecurity plan. Even if the IT group is responsible for the backup power system

cybersecurity plan, ensure that the cybersecurity plan includes the applicable *RPBP* ICS best practices such as the Zero Trust Security Model with multi-factor authentication and manual overrides of automated control systems.

- **Physical Security** – The facility's or site's physical security plan should attempt to mitigate intentional and accidental power system damage and theft. Fuel and small generators are often particularly vulnerable to theft during a prolonged power outage.
- **EM Security** – Consider adding mitigations to protect against intentional EM interference (IEMI) and EM Pulse (EMP) attacks. The *RPBP* provides very inexpensive and "rolling change" best practices for most critical infrastructure and more extensive mitigations for facilities that need an extremely high level of resilience.
- **Procurement and Installation Plans** – Discuss the procurement method (e.g., competitive, sole source) and who will perform the procurement. This should include an installation plan unless the project is very simple (e.g., install new surge protection devices). The installation plan should cover the equipment and accessories needed, the area(s) where the installation(s) will occur, installation milestones and any required regulatory or permits.

Some of the above may just reference other documents, including the *RPBP*. Based on the resilient power implementation plan, review the PMP again and update it as needed.

9 UPDATE OPERATIONS AND MAINTENANCE PLAN

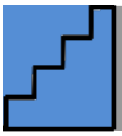
Resilient Power Team Preparation – Review existing Operations and Maintenance (O&M) Plan.

Poor maintenance is the #1 reason that generators fail when needed. In particular, insufficient fuel maintenance is the biggest cause of generator failures. Numerous other potential problems include not replacing a marginal battery, insufficiently weatherizing the equipment, and "wet stacking" (when unburned fuel passes into the exhaust system).

To help ensure that all of these issues are adequately addressed, the critical infrastructure organization should follow a well-regarded existing O&M plan or template and incorporate the *RPBP* O&M plan best practices. Some of the O&M sections to include are:

- **Planning, Organization, Equipment, Training, and Exercises (POETE)** should include regular audits of the POETE implementation per the O&M plan.
- **Technology-specific best practices** should leverage manufacturer O&M recommendations as well as industry best practices and the local environment.
- **Parts, tools, and supplies** need to be kept on hand in case it is not easy or quick to obtain these as discussed in the *RPBP*.
- **Diesel fuel maintenance and procurement** should be based upon contracts and not just performed on an ad hoc basis as noted in the *RPBP's Generators and Fuel* chapter. Unless regularly using your generator and replacing the fuel, properly maintaining the diesel fuel (or gasoline) is essential since bad fuel is often the leading cause of generator failures during power outages.

- **Load prioritization and efficiency** are important since these can reduce resilience costs while benefitting the environment at the same time. If implementing load prioritization, the prioritization details should be discussed along with any required manual operations.
- **Employee and contractor preparedness** should ensure that basic working conditions are taken care and that clean water, food, etc. are available. This preparedness may be part of a larger plan if it contains details specific to resilient power and considers the ramifications of employees, contractors, and vendors unable to travel to the site.
- **Laws and regulations** that impact the resilient power solution must be accounted for, including any POETE-related ordinances.

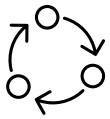


10 IMPLEMENT POWER AND O&M PLANS

Resilient Power Implementation Team – Read the facility's/site's resilient power plan and O&M plan.

Before implementing the resilient power plan, confirm that the plan will meet your organization's resilience goals and objectives and that the identified risks will be sufficiently mitigated by following the below steps:

- Review each power-related risk in your organization's risk management plan and ensure that each risk will be sufficiently mitigated.
- If there are any questions in the above review, use experts within or outside your organization combined with the resilient power team to build consensus that the identified potential issues will be sufficiently mitigated.
- When performing the above reviews, pay particular attention to your threat analysis and to systemic failures (e.g., flooding, extreme cold weather, cybersecurity attacks) that could occur across either the facility/site or other critical infrastructure sites that provide similar services.



Subsequently, implement the resilient power plan and then the O&M Plan. Consider using an iterative approach such as a spiral model particularly if some actions are far quicker, cheaper, and easier to implement than others. For instance, if the organization needs to improve its fuel maintenance program and replace an old, large generator with two new, smaller generators and a new load control system, consider quickly implementing the improved fuel maintenance plan before the new generators and load control system can be purchased and installed.

Follow best practices when procuring services from a third-party vendor or contractor. Ensure that the third party understands all the requirements that are applicable to their area of concern (e.g., this includes cybersecurity and EM requirements if procuring a power control system).

Lastly, document lessons learned in implementing this resilient power project and then periodically reassess your resilient power solution and validate that the existing solution continues to meet your resilient power needs. This includes ensuring that resilient power is part of any continuity exercises.

As facility requirements change, equipment ages, personnel changes are made, and new technologies become available or are more affordable, you may need to replace some of your equipment, update the facility's/site's resilient power plan, or improve the training.

CONCLUSION

These *Ten Steps of Resilient Power* provide an action plan to implement the CISA *Resilient Power Best Practices for Critical Facilities and Sites ("RPBP")*. Following the guidance in these documents can help improve critical infrastructure power resilience during short- and long-term power outages and can help the nation "withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks and threats to our economy and democratic system."[11]

Organizations should assign a resilient power champion and project leader who can then tailor these *Ten Steps* to the organizational needs and its budget. Both of these leaders should read these *Ten Steps* and read/browse the *RPBP* per the *RPBP's* Target Audience section.

Many organizations will want to perform some of the steps in a spiral model. For organizations that just want to implement a small part of the *RPBP* such as the generator and fuel maintenance suggestions, many of these steps can be bypassed.

Appendix A: ACRONYMS

ACRONYM	MEANING
ATS	Automatic Transfer System
BESS	Battery Energy Storage System
CCMG	Continuity Communications Managers Group
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity and Continuity of Operations
DHS	Department of Homeland Security
EM	Electromagnetic
EMP	Electromagnetic Pulse
EPA	Environmental Protection Agency
ESS	Energy Storage System
FEMA	Federal Emergency Management Agency
FMEA	Failure Modes and Effects Analysis
GMD	Geomagnetic Disturbance
HHS	Department of Health and Human Services

ACRONYM	MEANING
ICS	Industrial Control System
IRPF	Infrastructure Resilience Planning Framework
IT	Information Technology
NREL	National Renewable Energy Laboratory
O&M	Operations and Maintenance
PERT	Program Evaluation and Review Technique
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMP	Project Management Plan
POETE	Planning, Organization, Equipment, Training, and Exercises
REHS	Renewable Energy Hybrid System
RPBP	Resilient Power Best Practices for Critical Facilities and Sites
RPWG	Resilient Power Working Group
SMR	Small Modular Reactor
SPD	Surge Protection Device
UPS	Uninterruptible Power Supply
VoLL	Value of Lost Load

Appendix B: REFERENCES AND WEBSITE LINKS

1 https://www.cisa.gov/resilient-power-working-group
2 https://www.cisa.gov/resilient-power-working-group
3 https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit
4 PMBOK Guide | Project Management Institute (pmi.org)
5 https://www.cisa.gov/resilient-power-working-group
6 https://www.cisa.gov/resilient-power-working-group
7 https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit (11/17/2021)
8 https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf#
9 Department of Health and Human Services, Enterprise Performance Life Cycle Framework, Practices Guide, Project Charter (no date listed), https://www.hhs.gov/sites/default/files/ocio/eplc/EPLC%20Archive%20Documents/03%20-%20Project%20Charter/eplc_project_charter_practices_guide.pdf
10 Texas Department of Information Resources, Project Charter Template, https://dir.texas.gov/resource-library-item/project-charter-template
11 The White House, National Security Strategy of The United States of America (Dec 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf