Resilient Hospitals Handbook: Strengthening Healthcare and Public Health Resilience in Advance of a Prolonged and Widespread Power Outage[1]

Abstract:

A number of high-impact threats to critical infrastructure can result in a regional or nationwide months-long power outage, making it unlikely for timely outside help to arrive. Hospitals are encouraged to gain the capacity to make and store enough power on-site to operate in island mode indefinitely without outside sources of power or fuel and protect on-site capabilities from threats that could impact regional commercial power systems. This handbook outlines challenges and opportunities to solve these problems so hospitals, healthcare facilities, and other resources might become more resilient.

Introduction

In August 2005, Hurricane Katrina struck New Orleans and subsequently became one of the most destructive and expensive disasters in history. Hurricane Harvey's recovery costs in 2017 and beyond could be larger. Fortunately, disasters of this magnitude are rare, and some of the worst consequences may be preventable. Although loss of life has been statistically decreasing in domestic disasters (fortunately), the cost of disasters is skyrocketing. Some types of disasters, however, can still cause catastrophic loss of life. Disasters of the type discussed in this handbook may occur only once in a generation or even once in a lifetime.

Likelihood. The chance of just one type of these disasters occurring, extreme space weather in particular, has been described by various experts as having a likelihood of 6% to 12% in any decade.[2] A small number of high-impact, low-frequency (HILF) threats can deliver similar effects on their own. Any one of these threats or combination of threats may result in a widespread long-term collapse of critical infrastructure, which could minimize the ability of outside help to the affected communities. Although society has no way to stop natural hazards such as solar storms from occurring, there is much hospitals can do to minimize the consequences to their facilities. On the other hand, the chances of intentional man-made events decrease to the extent protections are in place and increase to the extent they are not in place.

Impact. According to various reports, including Lloyds of London[3], a 100-year storm could result in power outages lasting 1-2 years from DC to NYC alone[4]. Described as HILF events, they can even be existential in nature: for a particular business, for a specific hospital, for a community, or for a region. In

---

[1] The unrestricted general release of this report is in partial fulfillment of a Resilience Challenge in partnership with the National Institute for Hometown Security funded by the US Department of Homeland Security.

[2] See Pete Riley's article in Space Weather and abstract at: http://onlinelibrary.wiley.com/doi/10.1029/2011SW000734/abstract "the probability of another Carrington event (based on *Dst* < −850 nT) occurring within the next decade is ~12%."

[3] See the Lloyd's of London and AER 2013 report, "Solar Storm Risk to the North American Power Grid": https://www.google.com/search?q=solar+storm+Lloyds+of+London&oq=solar+storm+Lloyds+of+London&gs_l=psy-ab.3...613573.622915.0.623282.30.28.1.0.0.0.223.3091.3j19j2.24.0....0...1.1.64.psy-ab..12.17.2090...0j35i39k1j0i20k1j0i131k1j0i3k1j0i22i30k1j0i22i10i30k1j33i22i29i30k1.IoPK__ApmAo

[4] See impacts up to 1-2 years on coastal areas including the Gulf Coast and the Midwest.

turn, the severity of these threat scenarios compels local communities and institutions to be more resilient, so they can perform through these events and be in position to help their neighbors.[5]

Significance of healthcare. Of the 16 Critical Infrastructure Sectors[6] (as described in the National Response Framework), Healthcare and Public Health is perhaps the most fragile sector and is the most dependent on all the other sectors. Healthcare as practiced in the U.S. is complex and becoming more so as healthcare facilities become ever more dependent on technology, especially with regard to the U.S. power grid and information technology (IT). Hospitals cannot function without a steady uninterrupted supply of power and access to the digital world.[7] This handbook familiarizes and orients the reader to the subject of a prolonged and widespread power outage affecting all infrastructure sectors. However, the focus here is on threats to Healthcare and Public Health critical infrastructure, specifically hospitals and other large, fixed-base healthcare-related institutions. The purpose of the handbook is to help educate healthcare facility owners and operators (especially chief executive officers and their boards of directors) and other leaders on how to maintain resilience of their institutions throughout a high-impact event, specifically a prolonged and widespread power outage, in a cost-effective manner.

This handbook is *not* particularly focused on cybercrime, hacking, or cyberterrorism except as it relates to threats against the power grid. It will, however, address other scenarios that are typically beyond the scope of The Joint Commission Organization[8] review or a typical hazard vulnerability analysis. It is also *not* intended to be an exhaustive source of references on the subject of hospitals and disasters, nor will this handbook specifically address all requirements of the new Centers for Medicare & Medicaid Services' (CMS) Emergency Preparedness Rule.[9]

The handbook does, however, function as a checklist with a set of questions for the reader to address well before a disaster. The primary question is how to create, store, and use the power necessary to maintain essential functions and life safety for the hospital facility, which may be required to thrive and provide a surge of additional services in such a disaster. The five scenarios addressed here (i.e., cyberattack on the grid, extreme space weather, pandemic affecting a large percentage of the U.S. population, physical attack on the power grid, and electromagnetic pulse [EMP]) are unfamiliar topics for many hospital emergency managers. The common thread is how each of these scenarios affect the healthcare system, either directly or indirectly.

The handbook's content is specifically meant to be outside the usual set of challenges posed to hospitals in preparing for certain disasters and to stimulate new ideas and possible solutions. Hospital leaders can take some practical measures now to reduce loss of life and limit risk to their institutions in the event of a prolonged and widespread power outage, which are detailed later in this report. Preparedness efforts before a disaster facilitate a superior and much more cost-effective response than a response without

---

[5] These same actions can also create a more secure local economy and environment.

[6] https://www.dhs.gov/critical-infrastructure-sectors

[7] Water is also critical and deserves special attention as illustrated by Baptist Hospital in Beaumont, Texas, closed by lack of water during Hurricane Harvey. Water utilities are similarly dependent on power. Hospitals need to work with their water utilities to develop greater resilience and develop on-site alternative sources whenever possible, enhancing the benefits of microgrids using geothermal systems and pumped storage facilities as energy storage. In many cases, power may be the infrastructure with the longest lead time to repair and, hence, the more urgent to develop and protect from regional grid threats.

[8] www.jointcommission.org/

[9] www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep

adequate preparedness. Many of the solutions for high-impact threats can provide day-to-day benefits and resilience in the face of other unforeseen challenges.

Brief Overview of the U.S. Power Grid: How It Works and What It Looks Like

The North American power grid has been described as the largest and most complex machine in the world. Consisting of eight regional entities, it covers the bulk power supply of both Canada and the U.S. Within those regions are over 1,400 independent and semi-independent power companies under the oversight of two independent regulatory bodies—the Federal Energy Regulatory Commission (FERC) and the Nuclear Regulatory Commission (NRC)—as well as the Public Utility Commissions in each of the 50 states. To ensure coordination among the many thousands of power providers, the North American Electric Reliability Corporation (NERC) develops and enforces grid reliability standards. Power comes from a variety of sources: coal- and natural gas-fired utilities, nuclear, hydroelectric, solar, wind, and others. These power sources are connected by hundreds of thousands of miles of high-voltage and lower voltage electric lines. Balancing the loads and ensuring each jurisdiction is supplied according to the demand are functions of 16 NERC balancing authorities. Finally, the eight regional entities are grouped into three major regions in the U.S. and Canada: the Eastern Interconnection encompasses the area east of the Rocky Mountains and a portion of the Texas panhandle; the Western Interconnection encompasses the area from the Rockies west; and the Electric Reliability Council of Texas (ERCOT) covers most of Texas.

Transformers at the various substations first step up the voltage for efficient transmission of power across long distances and then again step down the voltage for use by customers. Most of the extremely large high-voltage transformers are custom made, weigh hundreds of thousands of pounds, are largely sourced from overseas, and are unique for their purposes. At various points in the distribution of electricity are monitoring and industrial control functions, some at remote locations. These are frequently unprotected industrial controls or automated Supervisory Control and Data Acquisition (SCADA) systems. These systems are often legacy devices that are accessible through the internet, embedded throughout the grid, and may not have been designed with common computer security measures in place. SCADA vulnerabilities are well known to the industry and make it possible for "hackers" to access essential grid functions.

Electromagnetic vulnerability. Intense solar activity (solar storms) has been shown to cause a reaction of the Earth's electromagnetic field electrifying the ground delivering electricity to travel along pipelines, rails, ground lines, and above-ground transmission lines; and inducing currents large enough to damage or destroy grid components (e.g., transformers). Although these storms may take hours to days to reach Earth, "turning off" the grid may not be possible or sufficient to avoid damage. Some types of readily available means of protection could be put in place to protect much of the grid against solar storms, but, for the most part, have not occurred.[10] Other physical phenomena associated with either nuclear EMP or non-nuclear electromagnetic weapons create frequency speeds in billionths and trillionths of seconds, faster than lightning arrestors function. These electromagnetic forces, arriving in nanoseconds, are much more destructive to electronics and require more sophisticated means of protection.[11]

[10] At the time of this handbook's preparation, various power grid elements continue to be tested by government and industry programs. Some utilities have begun to take efforts to protect portions of their infrastructure. However, the warnings of the Defense Threat Reduction Agency (DTRA) and others still stand.
[11] The military has been protecting some of its systems since the 1950s.

Physical vulnerability. Almost all of the large high-voltage substations and transmission lines are above ground. Some are visible to passersby and are often behind a chain-link fence. As such, they are vulnerable to physical attacks such as happened recently in California.[12] Finally, people ultimately control the power grid. Anything that prohibits employees to get to their places of work can affect the power grid.

Examples of Prolonged Loss of Grid Power to U.S. Hospitals

Hurricane Katrina, August 2005. What happened at Memorial Hospital in New Orleans, Louisiana, after Hurricane Katrina is instructive for what could happen elsewhere in the event of a prolonged power outage. One book, entitled "Five Days at Memorial: Life and Death in a Storm Ravaged Hospital,"[13] provides an emotionally engaging and in-depth picture of what it was like without electricity, running water, air conditioning, or supplies. To quote now from a *New York Times* August 2009 article[14] by Dr. Sheri Fink[15], "As at many American hospitals in flood zones, Memorial's main emergency-power transfer switches were located only a few feet above ground level, leaving the electrical system vulnerable." "'It won't take much water in height to disable the majority of the medical center,' said Memorial's CEO." What is interesting is that, unlike some other disasters affecting other hospital's building structure, Memorial was left mostly intact by the hurricane. Loss of emergency power was the critical feature. The Joint Commission requirement is for 96 hours of emergency power backup, but this typically only supports emergency lights, some equipment such as ventilators, and a few designated outlets throughout the hospital. The air conditioning system at Memorial shut down as did the elevators in the last few days of August. Supplies, food, and pharmaceuticals were all in limited supply afterward as the hospital was cut off by the floodwaters. After approximately 48 hours, the backup generator failed due to rising water and, sometime after that, potable water to the hospital also ceased. By September 1, "Dr. Pou was informed by the Tenet incident commander that 'no help was coming' and apparently the hospital was to be abandoned.".[16] As detailed in Sheri Fink's account, some patients lingered in these horrific conditions and ultimately succumbed to the heat.

The difference between Memorial Hospital and hospitals affected by Hurricane Katrina is that there was still the possibility of evacuation. Most of the patients in fact were successfully evacuated. Much of the effort directed toward saving patients was to transport them quickly to another facility by boat or helicopter. Evacuation of all patients was seen as the last best resort for a hospital that was failing. However, what if evacuation could not be accomplished due to lack of transport or lack of other functioning facilities within a reasonable radius? In a widespread and prolonged power outage, there

---

[12] One of the most well-known recent attacks was the one on the Metcalfe substation in April 2013 (see https://en.wikipedia.org/wiki/Metcalf_sniper_attack).

[13] See https://www.amazon.com/s/ref=nb_sb_ss_i_2_14?url=search-alias%3Dstripbooks&field-keywords=five+days+at+memorial+life+and+death+in+a+storm-ravaged+hospital&sprefix=Five+days+at+m%2Caps%2C224&crid=3OAEB5QWYKMFG

[14] See August 25, 2009 NYT Article, "The Deadly Choices at Memorial": http://www.nytimes.com/2009/08/30/magazine/30doctors.html?pagewanted=all&mcubz=1

[15] See this February 13,2016 NYT article challenging hospital preparedness in general, "Can Health Care Providers Afford to be Ready for Disaster?": https://www.nytimes.com/2016/02/14/sunday-review/can-health-care-providers-afford-to-be-ready-for-disaster.html?mcubz=1

[16] See the rebuttal of certain items in Dr. Fink's book by Dr. Pou at this website: http://www.memorialhospitaltruth.com/whathappened.html

would not be an evacuation option. Other medical facilities in the affected region would also plan to evacuate, but to where?

Super Storm Sandy, October 2012.[17] During Super Storm Sandy, more than 8.5 million households and businesses in the Northeast U.S. were without power from the grid. Hospitals in New York City had gone to great lengths before the storm to update and improve emergency power generation. For the New York University (NYU) Langone Medical Center[18], it was not enough. When sensors in the fuel tanks supplying those generators detected water from the storm, they shut down. Without emergency power, NYU Langone was forced to evacuate hundreds of patients to nearby hospitals. Emergency generators of all types, throughout the region, required refueling after several days and required maintenance to keep them running. Frequently, the same fuel suppliers were contracted to provide emergency fuel to many locations and were unable to keep pace with demand. When roads were closed and fuel was at a critical level, Department of Defense (DoD) assets were requested to provide relief.[19] Assets from as far away as California assisted, something far less likely during a nationwide prolonged power outage.

Although widespread, the power outage was not particularly prolonged for most customers. In this case, area hospitals were again called on to provide bed space for NYU Langone patients. Long lines of ambulances waited to take patients to nearby hospitals that still had power. The evacuation was deemed successful.

In a truly widespread and prolonged power outage, however, evacuation would not be an option. In addition, most hospitals already operate at or near capacity. Finding open beds, particularly for critical or trauma patients, is an almost daily struggle for some facilities. Worst-case scenarios for various disasters call for medical support for an additional 200,000 or more citizens in a major metropolitan area, thus requiring substantial surge capabilities and support from functional facilities.

Countering expectation. When threats impact the bulk of the country simultaneously, Federal Emergency Management Agency (FEMA), Department of Health and Human Services (HHS), Department of Homeland Security, and DoD capabilities are likely to be stretched thin and may not be available for a considerable time, if at all. In such situations, hospitals need to shelter in place or cease providing medical care altogether when a situation becomes untenable. Of course, it would be far better if every institution were so resilient they could continue to maintain close-to-normal capabilities and even meet the surge of additional demand that is likely in those circumstances.

---

[17] Sandy quick facts: Impacts Jamaica on October 19, 2012, and Atlantic City, NJ, October 29, 8.5 millions without power on October 31, half restored by November 1 (see Live Science at https://www.livescience.com/24380-hurricane-sandy-status-data.html).

[18] Since Hurricane Sandy, NYU Langone has developed considerably more resilient local power infrastructure, including a new combined heat and power system powered by natural gas. However, that system and the gas company supplying the natural gas are not EMP protected and remain vulnerable to many of the same threats facing regional grids.

[19] Fortunately for many, the U.S. DoD was able to supply necessary resources from around the country including the West Coast.

Possible High-Impact, Low-Frequency (HILF) Threats Affecting the Power Grid

Cyberattack on the U.S. power grid. This has already occurred and is very likely to occur again. In 2014, Russia tested a complex attack scenario (HAVEX/Black Energy2) against the American Grid. The attack primarily affected Industrial Control Systems (ICS) and SCADA devices. Subsequently, Russia was able to launch its improved version of the malware on the Ukrainian national grid, shutting down power to about 230,000 customers. The attack included a distributed denial of service attack on call centers. The attack did not damage expensive and difficult-to-replace equipment but rather demonstrated the ability to take complete control over the energy sector control centers. Much earlier, in 2007, Idaho National Laboratories demonstrated the ability of a cyberattack to cause physical damage (Aurora Test) to a diesel generator by opening and closing circuit breakers remotely. Since that time, cyber weapons have become increasingly sophisticated and countermeasures continue to be implemented but appear to lag behind the threats. The Secretary of Energy, under the FAST Act of 2015, cautions against minimizing the ongoing vulnerabilities of the U.S. energy sector to cyberattack.

Some steps to protect against cyberattack on the grid include concepts that could be applied to local power generation sources such as microgrids:

- Encrypt all control center communications
- Limit on-site access to data systems
- Require biometric means for access to certain areas
- Use two-factor verification for all systems
- Limit remote access
- Reduce equipment having a single point of failure
- Minimize internet access to SCADA and control systems
- Enhance cybersecurity on all systems
- Provide additional cybersecurity training to all employees
- Establish 24/7 cybersecurity monitoring
- Use only “whitelisted” equipment for SCADA and ICS
- Do not rely on “air-gapped systems” to remain offline

Solar storms or extreme space weather. This is a fascinating area that continues to motivate scientific investigation with substantial real world consequences for the power grid. In 1989, a relatively minor solar event interrupted power for over six million customers in Canada for at least nine hours. In 1859, the so-called Carrington Event struck North America with a walloping solar storm and induced a geomagnetic disturbance (GMD), which damaged telegraph lines and some telegraph stations across the continent. The sun randomly continues to produce coronal mass ejections (CMEs) sufficient to physically destroy much of the power grid the nation relies upon. The only defense so far has been that the Earth was not in the direct path that the directional CMEs could cause much damage.

What many may not realize is that, on July 23, 2012, the Earth narrowly missed a major coronal mass ejection from the sun by about nine days.[20] This was subsequently described as a Carrington-level storm that, according to estimates by Lloyds of London, could create a power outage lasting as long as 18 months from NYC to DC.[21]

Imagine if Earth had been hit by that massive solar storm in July 2012, only to be hit by Hurricane Sandy the following September, long before being able to recover from the larger power outage caused by the giant solar storm. Relatively little help would have been available outside the region affected by Sandy since many areas outside the hurricane-impacted area would have still been coping with their own difficulties.

Long-term "grid" vulnerabilities for solar storms include the destruction items requiring long lead times, including large transformers that transfer power across continental power distribution regions. Since transformers take over a year to build and procure, with few available spares, their destruction could result in extended lead times for custom replacements to be manufactured and reinstalled.

Hospital executives are usually not in the position to take measures to harden the bulk American power system, but they are in the position to make enough of their own power to maintain hospital operations. In fact, even when the regional power grids are protected from various threats, being overly dependent on centralized infrastructure is like putting all the eggs in a few giant technology baskets. It makes more sense for many reasons to diversify risk and increase resilience by making critical loads locally on or near a particular location.[22]

Electromagnetic pulse (EMP). EMPs result from a number of causes, the most impactful being a nuclear detonation in the upper atmosphere. High-altitude weapons testing in the 1950s and 1960s demonstrated the phenomenon could cause significant damage to electronic equipment, but without ionizing radiation, blast, or heat on the ground. Older technology (i.e., vacuum tube) was more resistant to the extremely powerful and extremely fast EMP than the microcircuits contained in virtually all modern devices. A single explosion (or several explosions) high above the U.S. could cover the country coast-to-coast. The commercial power grid is not yet EMP protected and remains a key vulnerability that could cause cascading effects to other systems, including communications, water, and healthcare facilities.

Coordinated physical attack on the power grid. This continues to be a significant threat. Although great strides have been made to ensure the electric grid's reliability, so too have the nation's adversaries who

---

[20] See https://en.wikipedia.org/wiki/Solar_storm_of_2012

[21] See https://www.google.com/search?q=solar+storm+Lloyds+of+London&oq=solar+storm+Lloyds+of+London&gs_l=psy-ab.3...613573.622915.0.623282.30.28.1.0.0.0.223.3091.3j19j2.24.0....0...1.1.64.psy-ab..12.17.2090...0j35i39k1j0i20k1j0i131k1j0i3k1j0i22i30k1j0i22i10i30k1j33i22i29i30k1.IoPK__ApmAo

[22] Some measures which could protect the power grid against extreme solar weather are:

- Install GMD monitoring and blocking devices at various select critical locations
- Provide additional spare equipment to selected substations
- Standardize major equipment to facilitate replacements
- Stockpile replacement transformers in select locations
- Shed load, if and when possible, to reduce transformer reactive power consumption and overheating

have sought to exploit inherent vulnerabilities. Although EMP, solar weather, and cyberattacks against the electric grid can be somewhat complex, a simple physical attack on a substation can have a similar impact. The vulnerable points to an electric grid physical attack include power generation plants, transmission lines, transformer substations, utility-owned communications systems, and industrial control facilities.

Most power generation plants are physically manned with defined defense perimeters such as chain-link fences and video camera monitoring. Notwithstanding security measures, successful physical attacks occur. One case in point is a sniper attack on the Metcalf Transmission Substation located in Coyote, California, near the border of San Jose. It occurred on April 16, 2013, when gunmen fired on 17 electrical transformers, which affected the greater San Jose area.[23]

Before the shooting, the attackers cut a series of fiber-optic telecommunications cables. It was a sophisticated and well-planned attack with the apparent intent of creating an extended electrical power outage in one of the nation's high-technology centers. The extended power outage, albeit targeted toward the area industrial complex, would have affected all electricity consumers, including hospitals. During the incident, a Pacific Gas and Electric (PG&E) technician was coincidentally performing testing on the electric grid and noticed an abnormality coming from the Metcalf substation. Had he not immediately implemented emergency procedures and had alternative routing capability, an extended and widespread electrical power outage, due to cascading failures of adjacent power stations, would possibly have occurred.

The incident was an eye-opening event for PG&E, which subsequently invested over $100 million to protect the substation against unauthorized entry. Unfortunately, the Metcalf substation was again breached in August 2014 and further damage to substation components was inflicted. To date, both breaches remain unsolved.

The Metcalf substation event illustrates the fact that events can and do happen outside an organization's control. The lesson to be gained is how best to prepared and build resilience to ensure organizational survivability and continuity of operations.

Pandemic (highly pathogenic influenza Type A). This seems to be the outlier in this HILF list. In fact, some experts believe a severe pandemic is a near certainty, "not if but when," in the next few decades. Extrapolating from the 1918 Influenza pandemic to today, approximately 90 million Americans would become ill (assuming a 30% attack rate), almost 10 million would need to be hospitalized, 1.5 million would need care at an intensive care unit, and 750,000 would need mechanical ventilation. Clearly, the capability is not currently available to care for such numbers. More to the point, it can be assumed that perhaps 50% or more of those who become ill would seek medical care. This would overwhelm existing capabilities, hence a recommendation for many persons with influenza-like illness to stay home unless the patient meets certain criteria.

DoD used a working estimate of 40% absenteeism from work during a pandemic[24] as the threshold for critical infrastructure to begin to fail. Many employees would remain home to care for a loved one or to

[23] See this 2016 article reviewing Metcalfe and concerns about similar attacks: https://www.eenews.net/stories/1060043920

[24] This includes work led by Dr. Terbush.

avoid getting the infection from co-workers. Employees of the energy sector (power grid) are no exception. When absenteeism hits 40%, it is estimated that sections of the power grid would go offline. When that happens, the scenarios of previous HILF threats and consequences for hospitals become the same or similar.

Some measures available to prevent and/or limit the spread of pandemic Influenza include:

- Routine use of hand-washing, cough hygiene, and social distancing measures
- Support for new rapid vaccine development technology
- Widespread distribution of (effective) anti-viral medications
- Consideration of school closures (children are more efficient spreaders of Influenza A)
- Limitations on large gatherings (e.g., conferences, shopping malls, church services)
- Telework (if available, telework has been shown to significantly decrease the spread of illness)
- Home care (stay at home if ill and avoid going to the hospital unless certain criteria are met)
- Prevention resources (e.g., CDC website, https://www.cdc.gov/flu/pandemic-resources/index.htm)

Other weapons of mass destruction. These can also function as high-impact threats to critical infrastructure but are not examined in this handbook. However, resilience that provides protection from high-impact threats covered in this handbook would provide benefits for other threats and scenarios that are not specifically addressed.

Recommendations for Protection Against All High-Impact Hazards Threats to Power Infrastructure

Although eliminating the risk of attack on the electric grid is impossible and outside the responsibility of any individual organization, it is possible to mitigate the indirect effects if (when) an attack against the electric grid were to occur. Hospital executives can enhance protection for a local hospital facility against attack on the electric grid by a variety of means such as:

Current Power Systems

- *Procure redundant power via electrical feeders from different substations and, if possible, different providers.* Receiving electrical power from different providers diversifies electrical power sources and thereby mitigates some risk.
- *Test generators under full load*. Many organizations test their generators on a monthly basis to determine if they will start and operate as desired. If diesel generators are repeatedly started but not under a full load, full output may not be realized when needed. Generators available to hospitals can include monitoring and testing systems to ensure they work when needed. In long-term power outages, diesel generators would still be useful but insufficient to guarantee power availability.
- *Enhance backup power generation*. Diesel generators are the most available and a proven source of backup power that should be maintained and exercised. However, they have severe limitations in an extended power outage scenario. Diesel generators must have sufficient backup power to meet critical mission areas. Equally important, facilities must have sufficient diesel fuel supply to endure for an extended power outage. Hospitals are required to have 96

hours of fuel, but seven days is a more realistic minimum standard for smaller day-to-day outages. If an extended power outage occurs, contracted fuel delivery would be assigned to the highest priority requirements and redirected by local and federal officials. In extended power outages, refineries may cease functioning and little fuel may be available at all. Fortunately, the infrastructure of backup power can be used to form the design basis of an on-site or near-site microgrid.

New Systems

- *Create an on-site (or near-site) power generation and storage capability incorporating on-site energy sources with an appropriate level of energy storage to provide the base loads required to keep the hospital functional (usually 30-50% of all power)*. Renewable energy such as wind, solar, and geothermal systems can diversify electrical energy sources and enhance resilience. The challenge is to have sufficient energy storage such as batteries to meet critical needs at all times. This solution (i.e., renewables and energy storage) can serve as an uninterruptable power supply (UPS) for the base load that can continue to operate through the power outage, thus allowing backup diesel generators to either be kept in reserve to support the microgrid or provide power over and above what the microgrids would provide in the case of a prolonged outage.
- *Consider energy savings from local power generation and energy efficiency improvements to help discover funding for new microgrids*. The energy produced by local microgrids can produce energy savings that can be used in power purchasing agreements that can help pay for the procurement of EMP-protected microgrids. Coordination with other energy efficient systems can further fund microgrids out of savings.
- *Consider natural gas-fueled generators*. Natural gas generators can provide a suitable alternative electrical power energy source. However, they may be vulnerable to a widespread electrical power outage, where natural gas pipeline pumps are powered from the electric grid. However, natural gas generators (usually in configurations as a combined heat and power [CHP] system) can be part of an overall power solution that can help fund the development of a more complete system, a portion of which can be more resilient than the unprotected CHP system.
- *Consider creation of EMP-protected facilities for power, network, and data center infrastructure*. The development of a control room for a new microgrid could be expanded to provide protection for other networking, data center, and security needs.
- *Consider developing a system-of-systems evaluation of the facility.* This would be similar to those supported by the NIHS program producing this handbook, which could provide technical and financial support necessary to enhance resilience in light of high-impact threats.
- *Consider inclusion of systems modeling and management.* This could aid in the development of a microgrid, help manage a microgrid after it is built, and assist in its ongoing development, including the potential to sell power in coordination with local utilities and support connecting and disconnecting from power grids.

All Systems

- *Bolster physical security*. Electrical feeder lines and backup power generation are often secondary considerations when considering physical security even though they represent key

vulnerabilities to operations. Security cameras and motion detectors should also be considered to bolster physical security measures and be part of an independent EMP-protected power and network management system that continues to function throughout a power and network outage.

- *Limit access to essential personnel*. As electrical feeders and backup power generation are critical nodes to operations, access should be limited to only trusted personnel who have a requirement to maintain and/or test facilities. All personnel with access to critical facilities (including custodial and contractors) should be screened with at least minimal background checks to minimize the potential for "insider threats."

Why Focus on EMP?

Focusing on an EMP is useful for a number of reasons. First, it can occur in more ways than most people are aware, and some EMP events can create the most widespread and long-term impacts to critical infrastructure such as power and water. Second, there are proven ways to address EMP through island-mode operation, which provides a helpful resilience model for facility owners and hospital managers.

It helps to understand that disruptive or damaging electromagnetic interference (EMI) can occur in a number of ways. Precautions against the harshest intentional manmade versions provide protection against the others. Nature provides its own versions from extreme space weather. Manmade EMI can be accidental or intentional.

Intentional EMI can come from small electronic weapons that can be carried in briefcases or larger ones that can be driven by van or truck. Now that capabilities of the weapons are increasing, it is possible to drive by a targeted control or data center and disable it without ever getting closer than a few hundred yards outside a security fence. Perpetrators could deliver damaging attacks without being noticed and continue to the next target (or come back another day). Motives for that kind of attack range from terrorism to sophisticated criminal actions (e.g., to short the stock of a targeted public company).

The most impactful EMP results from the detonation of a nuclear weapon 10-300 miles aboveground, which then creates electromagnetic fields that stream to Earth in all directions.[25] The higher the detonation, the larger the impacted area would be. Because there is no need for vehicle reentry into the lower altitudes or great requirement for accuracy, experts believe this could be an easier technology to develop or acquire for emerging nuclear powers as well as non-state actors. A small weapon detonated 80 miles high could affect a large multi-state region, whereas one detonated 300 miles over the center of the U.S. could affect the entire continental U.S. A ground-burst nuclear weapon would have a more limited radiated EMP, but an EMP that travels along conductors such as power lines could be more far-reaching and affect a larger area.

Both non-nuclear and nuclear EMP could disrupt or damage power generating stations, SCADA devices, computer equipment, and telecommunications networks. The proven ways to protect facilities from EMP include resilience of local facilities to operate in island-mode through the initial attack and until recovery is complete.

The likelihood and severity of either a nuclear or non-nuclear EMP attack was sufficiently large for the Defense Threat Reduction Agency (DTRA) to recently launch a request for proposals through the Small

[25] Even a small 5-10 kiloton weapon can create a significant EMP depending on emissions.

Business Administration program named the Small Business Innovation Research Program. The proposal seeks to create EMP-protected microgrids. In its official announcement and subsequent press release approved for unlimited general release, it stated, "An electromagnetic (EM) attack … has the potential to degrade or shut down portions of the electric power grid important to the DoD…. Restoring the commercial grid from the still functioning regions may not be possible" (See the RFP from DTRA)[26]. The DTRA goal was to "accelerate the adoption of EMP-protected critical infrastructure and microgrids among civilian institutions that need to operate in island mode during a prolonged power outage. These include… water utilities, hospitals and emergency communications."

A further risk is damage or destruction of micro-electronic circuitry in any of the various devices that people have come to heavily depend on for daily activities, especially larger items and those connected to wires of a meter or longer.[27] Medical devices in hospitals are not exempt from this effect. In addition to computers and communications equipment, IV pumps, bedside monitoring equipment, ventilators, etc. could be affected as all contain microchips. Again, the size, configuration, and connections at the time of a pulse are all factors.

In a dystopian novel based on a severe EMP scenario (i.e., "One Second After," by William R. Forstchen),[28] three public health crises occur as a result. The first is lack of ability to access medical care (i.e., hospitals, clinics) and lifesaving medicines (i.e., antibiotics, insulin). Persons who rely on electricity-powered devices to keep them alive (i.e., oxygen generators, dialysis machines) succumb without access to power. The second is a period of civil unrest, which is outside the scope of this discussion. The third is a return to preindustrial methods of food production, food distribution, and economic exchange. All three are associated with significant hardship and loss of life. In a worst-case scenario EMP, a one-year power outage (or even longer) would possibly occur before the majority of the power distribution network is restored.

---

[26] See text within RFP: https://www.sbir.gov/sbirsearch/detail/736859 " An electromagnetic (EM) attack (nuclear electromagnetic pulse [EMP] or non-nuclear EMP [e.g., high-power microwave, HPM]) has the potential to degrade or shut down portions of the electric power grid important to the DoD. While a power grid may employ intentional islanding techniques to protect sections of the grid and prevent a cascading collapse of the power grid, the broad reach of potential EM attacks with the potential of simultaneous levels of disruption might prevent traditional islanding protection methods from being sufficient for continued operations of the DCI. Restoring the commercial grid from the still functioning regions may not be possible or could take weeks or months. Significant elements of the DCI require uninterrupted power for prolonged periods to perform time-critical missions (e.g., sites hardened to MIL-STD-188-125-1). To ensure these continued operations, DCI sites must be able to function as a microgrid that can operate in both grid-connected and intentional island-mode (grid-isolated). Such a microgrid is defined as a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the power grid."

"

[27] Another considered risk is that modern automobiles contain many microchips. In an EMP event, these microchips may stop the engine from running or even fail to start at all, especially if connected to a wiring system that would make it possible for the electromagnetic currents to couple with them. Changes in the use of automobile electronics, configuration, wiring methods, and auto body materials would all impact the likelihood and amount of impact for any particular vehicle. (*Note:* DoD funded the development of EM devices mountable in helicopters to disable automobiles driven on highways.)

[28] See the series of books by Dr. Forstchen at https://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Dstripbooks&field-keywords=One+Second+After&rh=n%3A283155%2Ck%3AOne+Second+After

Characteristics of Resilient Hospitals

Beginning with Homeland Security Presidential Directive 21 (HSPD-21) and followed by Presidential Preparedness Directive 21 (PPD-21), federal level planners have increasingly used the term "resilience." Resilience as an operational concept, however, has been around a long time. As a point of reference, "continuity of operations" can be used almost interchangeably. For the purpose of this handbook, a shortened definition of resilience is "the ability to take a blow and come back." The Joint Commission (JCO) established a baseline for emergency preparedness for hospitals and other healthcare institutions.[29] Although the specific requirements for the Healthcare Organizations' evaluation are available for purchase from The Joint Commission, there is a wealth of detailed helpful information on the JCO website for hospitals to become more disaster resilient.[30]

The CMS/HHS Final Rule for healthcare organizations also establishes national emergency preparedness requirements for Medicare- and Medicaid-participating providers and suppliers.[31] These requirements help providers and suppliers plan adequately for both natural and man-made disasters, and coordinate with federal, state, tribal, regional, and local emergency preparedness systems. Requirements are set for emergency power generation at many types of healthcare facilities within the Final Rule.

The HHS Sustainable and Climate Resilient Healthcare Facility Initiative is useful not only for weather emergencies but for disasters of many types.[32] This online document and toolkit provides a broad look at healthcare facility resilience. Although primarily focused on disasters related to climate change and severe weather, the steps recommended for healthcare facilities to take to improve resilience would be appropriate and useful for any of the five HILF scenarios. The toolkit is divided into various elements with Element #3 being Infrastructure Protection and Resilience Planning. Element #3 is further divided into the following "Steps": energy and utility infrastructure, energy conservation, water supply, water usage, sewage and wastewater, communications infrastructure, and medical information infrastructure. The document also introduces the term "islanding."

Resilient community islands. The concept originally began with the energy sector and the necessity of being able to "black start" some power stations (i.e., restart power stations after a widespread power outage). This in turn would help to bring larger sections of the power grid back online. The term "resilient community islands" has since been used to refer to resilient organizations: university campuses, state and local governments, military bases, and certain critical businesses, which each continue their essential functions and remain in communication with other "islands." Another example of a functionally differentiated community island would be a medical campus/hospital. If the hospital had its own power supply and other essential resources (e.g., water, food, and communications), it could be a focus for medical care for other functioning islands and possibly help to bring other medical facilities back online.

Graceful degradation. The concept of "graceful degradation" of services is not new. Continuity of operations plans have long been developed to maintain essential services and to eliminate nonessential

---

[29] Joint Commission (JCO) requirements can be found at: https://www.jointcommission.org/emergency_management.aspx

[30] https://www.jointcommission.org/assets/1/6/US_National_Library_of_Medicine_-_Disaster_Health_Information_Resources_052014.pdf

[31] https://www.federalregister.gov/d/2016-21404

[32] https://toolkit.climate.gov/topics/human-health/building-climate-resilience-health-sector

ones. This concept includes the idea that, in a widespread and long-term power outage, hospitals may need to continue to provide the most essential services for as long as possible and then have a plan for which services must be eliminated. Resilient hospitals have plans in place to fail gradually and not catastrophically (fragile systems). This requires thoughtful analysis of a particular facility's mission as well as the particular needs of the community the hospital serves.

Electricity is, of course, not the only critical resource needed to maintain hospital operations. Other critical infrastructures affecting hospitals include water and wastewater and sewage removal. In fact, water may be even more essential to hospital operations than electricity. A hospital would lose the ability to provide essential functions almost immediately if the water supply is interrupted when the grid goes down. Some specific requirements such as loss of clean laundry also have a disproportionate negative effect on hospital functioning. Other critical infrastructure sectors affecting healthcare include: communications, emergency services, transportation, manufacturing, etc.[33] A case can be made that all of the other critical infrastructure sectors affect the Healthcare and Public Health sector.

The most critical resource for maintaining hospital operations is the human resource. A 2015 study was conducted using a variety of different disaster scenarios that asked the question, "Will hospital staff come to work?"[34] The results were perhaps surprising and disappointing. The most commonly cited reason for not coming to work was concern for family. Analysis of staffing needs (essential vs. nonessential) and possible mitigations (accommodations for families and pets) go a long way to improving hospital resilience. Some recommend having a requirement to respond in a disaster written into the staff employment agreement. Others rely on the "culture" of healthcare providers to positively respond in an emergency. A candid discussion with medical and non-medical staff in advance may also improve response.

Importance of Community Partnerships, Networking/Sharing of Essential Services

None of these resilience measures would be as effective if done in isolation. All of these measures benefit from collaboration with other organizations in the healthcare sector and other community members. The Joint Commission specifically looks for preparedness measures (risk management) within a community context. Healthcare coalitions are particularly valuable for community assessments and making progress toward resilience. Information sharing is key, both before and during the emergency. Identification of potential risks (hazard vulnerability analysis) in collaboration with community partners is essential. Healthcare institutions must know their role(s) in community, county, and regional disaster plans, during the planning and response. A mutual understanding of the vulnerabilities of the other critical infrastructure systems is more valuable that just looking at healthcare vulnerabilities alone.

In addition, there are often economies of scale when it comes to preparedness. Cyber- and EMP-protected microgrids may be more economically feasible when shared among several institutions on a healthcare campus. Purchasing agreements for contingencies may be complicated by the fact that numerous other users also have contracts and even (upstream) priority arrangements, such as the U.S. government. Competing contracts for diesel fuel, for example, became a critical resource that had a negative impact during Superstorm Sandy. Fuel stored in underground tanks is unavailable in a power outage, unless a separate generator is available.

[33] https://www.dhs.gov/critical-infrastructure-sectors
[34] https://www.ncbi.nlm.nih.gov/pubmed/25807865

Finally, if an extended power outage were to occur, hospitals could expect a surge in activity when they themselves are operating under adverse conditions and less able to provide services. A hospital's reputation is dependent upon being able to provide services when its community is in need.

What Is a Microgrid? Why Be EMP-Protected?

To keep a hospital from shutting down during a prolonged power outage when backup generator fuel is unavailable, the hospital needs to generate and store enough power on-site to maintain core functions. But, it can only do that if the local power system is protected from the same causes that could lead to the failure of the commercial power grid.[35] For this reason, the DTRA asked for the development and deployment of EMP-protected microgrids for both military bases and the hospitals they use. DTRA recognizes commercial power grids are not designed to withstand electromagnetic threats and proposes local power systems be EMP protected and capable of operating in island mode.

A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously (i.e., "islanding").[36] Islanding is not the most challenging or difficult operational mode.

The two most difficult operational modes are: (1) the parallel operation with the grid, which has the highest value (both technically and economically); and (2) the ability to have that system be EMP-protected so, in an EMP event, the microgrid continues operating without damage or disruption by immediately detaching itself from the grid and operating in island mode indefinitely until the commercial power grid is restored. During normal operations, knowing when NOT to island is most important to overall grid stability and performance. On the other hand, a no-notice EMP event can damage the grid, its control systems and the hospital infrastructure it serves within nanoseconds without the knowledge of grid operators. This makes it necessary for EMP-protected systems to continue to operate through and after an EMP attack in island-mode even while the larger grid ceases to function after becoming one of the conductive pathways of damaging EMPs (see the DTRA press release for official comments on this threat and related IEEE[37] and military standards[38]).

---

[35] Minimizing exposure to EMP and cyberthreats from the earliest design stages can minimize the cost of protection.

[36] Smaller microgrids, sometimes known as nanogrids can be operated off-grid without a grid connection.

[37] IEEE Standard 2030.(7)/.(8) is in development at this time and will address establishing a standard for the Microgrid Energy Management System (MEMS) to enable interoperability of the different controllers and components needed to operate the MEMS through cohesive and platform-independent interfaces. The standard includes the control functions that define the microgrid as a system that can manage itself, and operate autonomously or grid connected, and seamlessly connect to and disconnect from the main distribution grid for the exchange of power and the supply of ancillary services. Additionally, the standard addresses the technical issues and challenges associated with the proper operation of the MEMS that are common to all microgrids, regardless of topology, configuration or jurisdiction, and to present the control approaches required from the distribution system operator and the microgrid operator.

[38] MIL STD 188.125 is an example of a military standard that can readily be applied to small on-site microgrids, control rooms and communications networks inherent in a microgrid. DHS has provided guidance based on that standard. (Large regional microgrids have additional complexities within its generation and transmission system that require additional work.) See: http://www.stop-emp.com/Final-DTRA-IAN-Press-Release%20-w-logos-centered.pdf

Power modeling and management software, combined with network management systems, can provide the foundation for a microgrid that provides resilience from EMP and cyberthreats. It also makes it possible to monitor systems so they can recover quicker from disruptions.

The technical advisors to this handbook propose a microgrid plan that takes industry and military standards into account and recommends a microgrid system capable of meeting those standards and ultimately capable of operating either in grid and island mode.

Potential power savings/cost savings. Hospitals can fund a substantial if not all of the costs for EMP- and cyber-resilient microgrids from a combination of energy savings and energy efficiency. Additional funding might come from projects that create mutual advantages between hospitals and their strategic partners, including those who may wish to conduct further applied research in this area. The financial advantage of a microgrid is that it can operate the base power load of hospitals on a day-to-day basis while reducing the spending for that amount of power from outside utilities. Furthermore, when a utility-based power outage occurs, the hospitals can shed loads that are not essential while continuing to operate their microgrids. Emergency generators would only need to continue operation activities beyond essential loads or be held in reserve in case of any other technical difficulties. By providing their own power for essential loads (i.e., often 30-50% of the entire power requirement), hospitals can use the savings from that portion of their power bills to fund the growth of their own systems. In many cases, though, the cost savings of local energy generation and storage may not be large enough to completely fund a microgrid. In these cases, it would be beneficial to find additional savings in energy efficiency measures so those savings could also be applied to the overall financial requirements for the on-site microgrid.

Additional reasons for on-site energy/power storage. On-site energy storage can provide cost savings that help fund the microgrid and the ability to continue functioning during a long-term power outage. It is also possible to develop a microgrid system that simultaneously serves other functions. The initial microgrid can be used to gather data to substantiate additional energy savings and performance advantages. That same data can assist in choosing the best microgrid power generation and storage elements for specific hospital requirements, environments, and utilities that it might connect. It can be used as a facility-wide power-management system that helps operators recover sooner after an infrastructure interruption or failure. It can also be used to support EMP-protected data and facility security system elements. These goals are best served when power monitoring and modeling software assist in these tasks with the support of professional engineers.

Preliminary microgrid assessments can be accomplished to create an initial EMP-protected microgrid that can be grown over time as the initial microgrid system provides data that support the self-funding for microgrid expansion.

How to Conduct a "Lights Out" Exercise

"Lights Out" was the name of a tabletop exercise conducted to explore the consequences of a long-term widespread power outage on a local hospital. A number of subject matter experts provided background information, including speakers from: NOAA's Space Weather Prediction Center, the U.S. National Renewable Energy Labs, public safety, public health, local (county) government, and the military. The scenario used was one in which a severe space weather event was followed by an opportunistic cyberattack on the power grid. This scenario was thought to be plausible and had been vetted in the

past. Short vignettes representing several days of elapsed time were followed by a series of questions for participants. The scenario, vignettes, and questions are contained in the attached documents at the end of the handbook. Speakers familiar with these subjects may be available for future exercises from InfraGard EMP-SIG, by contacting igempsig@infragardmembers.org or the Protective Security Advisor program at the U.S. Department of Homeland Security (https://www.dhs.gov/protective-security-advisors).

Appendices and Diagrams

Checklist for Hospitals in Advance of a Prolonged/Widespread Power Outage[39]

- ◊ What are the essential functions of your hospital in day-to-day operations? During an emergency? During an emergency or power outage lasting more than 30 days?
- ◊ What items from your entire supply chain need to be stocked locally? Have they been prioritized? Power is an example of what would be the most important and difficult to replace. Which others take longer to replace?
- ◊ Have you considered the use of on-site, renewable sources of electricity (solar/wind), geothermal, etc., as well as battery storage or similar energy storage system? What protection levels have they been certified from threats such as EMP and cyber attacks?
- ◊ Are priority areas/functions supplied by an EMP and cyber resilient microgrid or emergency power outlets/circuits? Partial or complete?
- ◊ Are your emergency generator(s) sufficient? How long can you continue to provide power to support essential functions without refueling?
- ◊ Are your generators sufficiently "hardened" to be able to withstand a weather emergency? A minor earthquake? Solar storm? Cyberattack? EMP? Physical damage from outside/inside your facility?
- ◊ Are the circuitry, panels, fuel tank sensors, and generators themselves, all protected from flooding damage?
- ◊ Is your plan for refueling emergency generators guaranteed and not subject to upstream requirements?
- ◊ Are you able to service a single generator (filters, oil) while keeping essential services online?
- ◊ Do you have external connections already in place for additional emergency generators?
- ◊ Are your heating (and cooling) systems on emergency power? Are there methods in place to transport patients within your facility, not electricity dependent? Is food refrigeration on emergency power?
- ◊ Are water distribution systems dependent on electricity to maintain pressure? Can you supply your water needs with a storage tank (or well) and emergency power generation? Do you have a way to purify that water if needed?

[39] For the complete HHS Sustainable and Climate Resilient Healthcare Facility Initiative Element 3 Checklist, visit https://toolkit.climate.gov/sites/default/files/SCRHCFI%20Checklist%203%20081415_Form.pdf

- ◊ Do your wastewater and sewage systems continue to function during a power outage? Do you have a means of preventing backflow of sewage into your facility, if required?
- ◊ Do you have several means of redundant communications, not dependent on grid power or a functioning internet? Do other healthcare facilities in your area have similar means/capabilities?
- ◊ Can your accounting/billing, electronic medical records, and data storage continue to operate? Is there off-site backup on emergency power or onsite microgrids independent of remote resources?
- ◊ Are you able to transition to a paper system for essential record keeping functions?
- ◊ Have you arranged "come to work requirements" with essential clinical and nonclinical staff and made provision for their transportation, food and sleeping arrangements, child care, pet care, elder care, etc.

Additional Resources and References for Resilient Hospitals Handbook Users

Hospital Emergency Preparedness and Response during Super Storm Sandy: https://oig.hhs.gov/oei/reports/oei-06-13-00260.pdf

Disaster Information Management Research Center (DIMRC): http://disasterinfo.nlm.nih.gov

InfraGard National EMP Special Interest Group (sponsored by the FBI) Publications with linked bibliographies

Triple Threat Power Grid Exercise: https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Dstripbooks&field-keywords=Triple+ThreaT+Power+Grid+Exercise

Powering Through, From Fragile Infrastructures to Community Resilience: https://www.amazon.com/Powering-Through-Infrastructures-Community-Resilience/dp/0998384402

High-Impact Threat Series of Conference Proceedings References

Planning Resilience for High-Impact Threats to Critical Infrastructure: Conference Proceedings InfraGard National EMP SIG Sessions at the 2014 Dupont Summit: https://www.amazon.com/Planning-Resilience-High-Impact-Critical-Infrastructure/dp/1633912612/ref=sr_1_3?s=books&ie=UTF8&qid=1503608965&sr=1-3&keywords=High+Impact+Threats

Engaging Communities for High-Impact Threats to Critical Infrastructure: Dupont Summit 2015 Conference Proceedings of the InfraGard National EMP SIG Sessions: https://www.amazon.com/Engaging-Communities-High-Impact-Critical-Infrastructure/dp/1633914291/ref=sr_1_6?s=books&ie=UTF8&qid=1503608965&sr=1-6&keywords=High+Impact+Threats

Mitigating High-Impact Threats to Critical Infrastructure: Conference Proceedings of the 2013 InfraGard National EMP SIG Sessions at the Dupont Summit:

https://www.amazon.com/Mitigating-High-Impact-Threats-Critical-Infrastructure/dp/1633911330/ref=sr_1_4?s=books&ie=UTF8&qid=1504540374&sr=1-4&keywords=high+impact+threats

High-Impact Threats to Critical Infrastructure: Emerging Policy and Technology: https://www.amazon.com/High-Impact-Threats-Critical-Infrastructure/dp/1935907395/ref=sr_1_1?s=books&ie=UTF8&qid=1504540374&sr=1-1&keywords=high+impact+threats

Contributors

Charles (Chuck) Manto, President Instant Access Networks, Chair EMP Special Interest Group InfraGard (cmanto@stop-EMP.com); Earl Motzer, Ph.D., Chair, Healthcare and Public Health Sector Coordinating Council; Art Glynn, CAPT USN (Ret.), Navy Emergency Preparedness Liaison Officer, FEMA Region 8, and Consultant with Booz Allen; James Terbush, MD, MPH, Public Health Instructor and President, Innovative Health Systems Inc.

Acknowledgments

We wish to thank Catherine Feinman, Editor-in-Chief, www.DomesticPreparedness.com; and, staff of the Policy Studies Organization, for their review of this document. We also wish to thank staff at Doctors Community Hospital in Lanham, MD; the University of Kentucky Medical Center in Lexington, KY; St. Francis Hospital in Colorado Springs, CO and the Society for Disaster Medicine and Public Health for their participation in hospital microgrid assessments and conferences on these topics that have helped inform this handbook. We are especially grateful for the offices of the state of Maryland that have also provided facilitation on these issues impacting hospitals and the National Guard that include the Maryland Emergency Management Agency, the Maryland Governor's Office of Homeland Security and the Maryland Department of General Services, especially the active involvement of Deputy Secretary for Energy Leigh Williams, Esq.

About FBI InfraGard and the Electromagnetic Pulse Special Interest Group (EMP SIG)

The Federal Bureau of Investigation's (FBI) InfraGard is a partnership between the FBI and members of the private sector to help protect the nation's infrastructure. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure.

The EMP SIG Mission is to facilitate information sharing and subject matter expertise nationwide to serve local communities so that they may become more resilient in light of threats that would lead to catastrophic, cascading losses of life-sustaining infrastructures and resources.