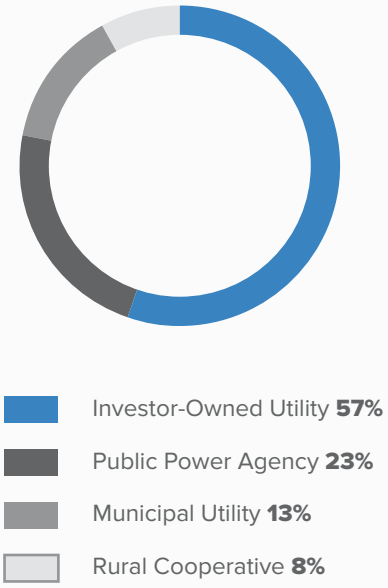
THE STATE OF PHYSICAL GRID SECURITY

2015

DEMOGRAPHICS

Every utility is different, so we asked those surveyed to provide information about the type of utility they work for, the grid operations their utility is tasked with and the size of their service territory.

What type of utility do you work for?



What is the electric customer base for your utility (number of customers served)?

Under 500,000	**30%**
500,000 to 1 million	**15%**
1–2 million	**19%**
2–4 million	**11%**
4 million or more	**24%**

EXECUTIVE SUMMARY

Every year, the nation's electric grid faces a myriad of physical threats — natural disasters, equipment failure, accidents, solar flares, and even planned acts of sabotage. Because these vulnerabilities can result in extended power outages that have severe economic consequences, physical grid security has become a principal concern for utilities and regulators.

To better understand the threats utilities face and how the grid's most critical assets are being safeguarded, Utility Dive conducted a survey produced in partnership with ABB, a leader in power and automation technologies, of more than 200 U.S. electric utility executives to understand how their utilities are addressing physical security.

In the aftermath of the FERC report that exposed the U.S. power grid's vulnerabilities, physical security has become a **growing concern for utilities and policymakers.**

Here are the key findings from our survey:

- The biggest challenge for utilities taking actions to improve physical grid security is an uncertain or difficult path to cost recovery.
- While most utilities have identified their critical substations and taken steps to assess potential vulnerabilities and threats to comply with NERC CIP-014, 28% say they have not yet completed any further initiatives.
- Natural disasters and aging infrastructure are considered the most severe threats for physical grid security.
- A large percentage of respondents (40%) indicated their utility has not taken any hardening actions in the last two years to delay or limit damage of their critical assets from physical threats.
- One of the biggest challenges for utilities recovering from major events is replacing large power transformers. Most utility executives surveyed believe that a national Strategic Transformer Reserve program is an important or critical need.
- Utilities are planning a variety of approaches to hasten recovery from major events, including stockpiling equipment, benchmarking best practices with industry groups, hardening substations, and developing rapid recovery plans.

The results of the survey indicate that while utilities are taking many steps to detect and deter physical security threats, preventing damage and recovering quickly remain significant challenges for the industry.

THE STATE OF PHYSICAL GRID SECURITY

THE NATION'S ELECTRIC POWER IS DELIVERED through a complex network of generating stations, substations and transmission lines. Large power transformers at high-voltage (HV) substations, which step up and synchronize voltage for transmitting electricity long distances over power lines, are among the most critical assets for utilities. Although these HV transformers account for less than 3% of all substation transformers, they carry nearly 70% of the nation's electricity. The critical role that these HV transformers serve underscores the potential for widespread outages if even a small number are damaged or disabled.

Recent events have demonstrated that the electric grid faces increasingly frequent and new physical attacks. Severe weather — such as Hurricane Sandy, which knocked out power to nearly 9 million people for days and sometimes even weeks in 2012 — presents the most common physical threat to substation assets. However, utilities have reported over 300 intentional physical attacks on grid infrastructure between 2011 and 2014 that resulted in power disturbances, including a coordinated malicious attempt to disrupt power by firing more than 100 rounds of ammunition at a substation's transformers.

These attacks raised serious concerns in the industry over the physical security of the power system. A subsequent analysis by the Federal Energy Regulatory Commission (FERC) found that the sabotage of just nine critical substations could lead to coast-to-coast blackouts lasting 18 months or more.

FERC report: The sabotage of just nine critical substations could lead to coast-to-coast blackouts lasting 18 months or more.

To address these concerns, FERC directed the North American Electric Reliability Corporation (NERC) to establish Critical Infrastructure Protection (CIP) standards for physical grid security, known as CIP-014. The CIP-014 standards, which went into effect on January 26, 2015, require utilities to conduct a risk assessment to identify critical facilities, evaluate potential threats and vulnerabilities, and implement a security plan to protect against potential attacks on critical facilities. As utilities have begun identifying their critical grid assets, many see regulatory and institutional challenges for implementing protective measures.

RECOGNIZING VULNERABILITIES

In recognition that a physical threat to only a small number of critical substations could cause widespread and extended outages, NERC CIP-014 requires utilities to conduct an initial risk assessment and identify critical facilities — typically those above 200kV — that if rendered inoperable or severely damaged could result in significant power system problems and even cascading failures. For the overwhelming majority of small utilities — those with fewer than 500,000 customers — respondents said less than 25% of their substations are critical. Respondents from mid-sized utilities with 1-2 million customers have a larger percentage of critical facilities, with 40% reporting that between 25-50% of their substations are critical. Large utilities that serve over 4 million customers have dramatically higher percentages of critical substations: One-third of large utility respondents reported that more than 50% of their substations are critical, while one-in-five large utility respondents indicated that more than 75% of their substations are critical. While complete protection of every substation and transformer may be difficult to achieve, securing the most vital assets will have the biggest impact on protecting grid reliability.

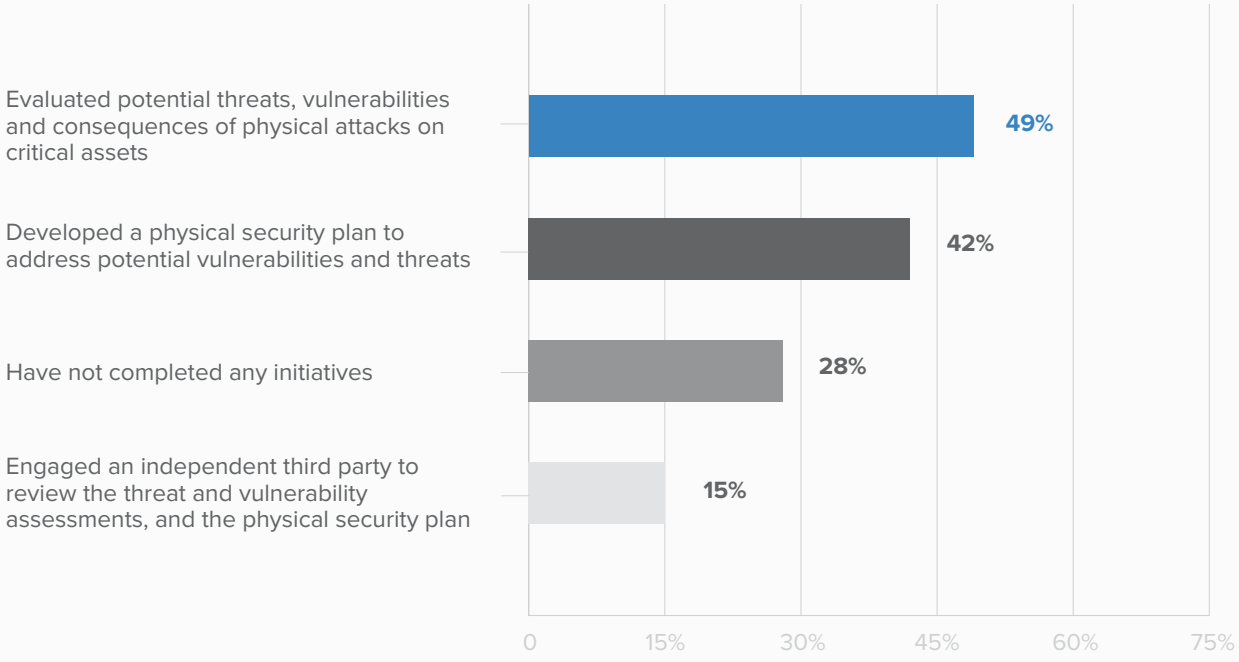
Approximately what percentage of your substations are considered critical under NERC Critical Infrastructure Protection (CIP)-14 physical security requirements (typically those substations operating above 200kV) and require additional physical security planning?

Less than 25%	**47%**
26% to 50%	**27%**
51% to 75%	**15%**
76% to 100%	**11%**

According to survey respondents, utilities are in various stages of meeting CIP-014 requirements. Nearly half of respondents indicated their utility has evaluated potential threats, vulnerabilities and consequences of physical attacks on their critical assets. 42% said they have developed a physical security plan to address these vulnerabilities and threats. Some have even progressed to engaging an independent third party to review their threat and vulnerability assessments and the physical security plan. But although most utilities are well underway with complying with NERC CIP-14, nearly one-third of utilities surveyed have not yet completed any initiatives.

Almost half of the utilities surveyed have already performed vulnerability assessments, **42% have already developed physical security plans.**

What steps has your utility undertaken to comply with NERC CIP-14 requirements for physical security of transmission substations? (Select all that apply)



DETECTING AND DETERRING THREATS

A strategic component of physical grid security is taking steps to detect and deter threats. In this regard, utilities are relying less on personnel and more on automated systems. While 25% of surveyed utilities have increased the presence of on-site security personnel, the majority (74%) have undertaken measures to restrict physical access at substations, such as the installation of card readers, automated gates, smart locks and unique keying systems to restrict access to only authorized personnel. Remote electronic surveillance equipment such as closed-circuit monitoring, thermal imaging (i.e. infrared cameras), acoustic sensors and motion detectors are used by 60% of respondents to monitor their critical assets for unauthorized access and potential threats. Alarm systems that monitor for unauthorized access, tampering or forced intrusion are used by 65% of utilities surveyed, and one-quarter are even using advanced communication software and analytics to monitor the condition of substation equipment. A much smaller percentage (4%) use aerial drones for monitoring.

What types of operational or monitoring measures has your utility implemented in the last two years to detect and deter physical security vulnerabilities and threats at transmission substations? (Select all that apply)

Limited access to authorized personnel through techniques such as installation of card readers, automated gates, smart locks, and/or other unique keying systems	74%
Deployed alarm systems to monitor unauthorized access, tampering, or forced intrusion	64%
Utilized remote surveillance equipment such as closed-circuit monitoring, infrared cameras/thermal imaging, acoustic sensors, motion detectors, or other electronic monitoring devices	58%
Assessed potential threats using advanced communications software and analytics to monitor the condition of equipment	25%
More on-site security presence by increasing the number or frequency of patrols, number of guards on-site at any given time, and/or footprint of areas patrolled	25%
Other	6%
Used aerial drones for inspection and monitoring	4%

What design modifications has your utility made in the last two years to deter physical security threats at transmission substations? (Select all that apply)

Installed physical barriers including fencing, perimeter walls, or locks	**60%**
Enhanced substation lighting, vegetation, or other measures to manage visibility of assets and detect threats	51%
Relocated spare equipment to off-site storage areas	22%
Reconfigured transmission stations to limit the impact of a single event	21%
No modifications have been made	20%
Camouflaged substation equipment through enclosure or placing assets underground	9%

Another way utilities are addressing physical security is to make design modifications to shield substation assets from threats by using protective and visual barriers. Because of their large physical size, HV transformers are vulnerable to intentional attacks. Most utilities surveyed (60%) have installed physical barriers such as fencing, perimeter walls and locks around their substations. Measures to manage visibility of substation assets and allow easier detection of threats, such as lighting and vegetation are used by half of utilities. Some respondents say they have even taken steps to reconfigure their substations to limit the impact of a single event (21%), relocate spare equipment to off-site areas (22%), and camouflage or hide equipment underground (9%). But 20% of those surveyed have not yet made modifications to deter threats.

The main design modifications that many utilities have made over the last two years to detect and deter threats at their substations are **installing physical barriers and taking measures to manage the visibility of critical assets.**

DELAYING IMPACTS

Making substation equipment more resistant to physical damage from intentional attacks, accidents or extreme weather is called hardening. Hardening measures are intended to delay impacts and limit damage. Utilities have undertaken various approaches for hardening their critical substation equipment, from measures to prevent the spread of fires and ballistic shielding to hardening communications and control systems. Substation fires may be caused by electrical short circuits, ignition of transformer oil, and acts of sabotage. One-fifth of utilities are attempting to reduce fire risk by using less flammable oil.

Due to the important role served by communications in detecting physical threats, 32% of respondents indicate their utility has taken action to strengthen the resiliency of communications equipment and nearly 25% have hardened control houses. Nearly 40% of respondents have not undertaken any hardening actions in the last two years. This is an indication that utilities are taking a phased approach to physical security. Utilities are starting with the low-hanging operational measures, whereas hardening – which takes longer and is saddled with a longer path to cost recovery – comes later in the phased approach.

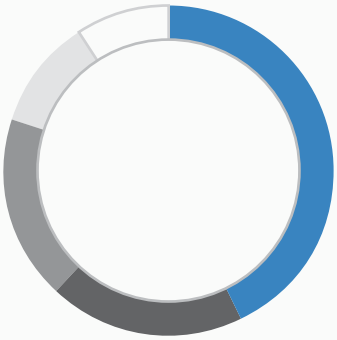
What types of hardening actions has your utility taken for transmission assets in the last two years to delay physical security threats? (Select all that apply))

No actions have been taken	**39%**
Strengthened the resiliency of communications	**32%**
Hardened control houses	**24%**
Used less flammable oil in substation equipment	**20%**
Installed armor or ballistic shielding of transformers and other HV equipment	**12%**
Installed redundant cooling systems	**12%**
Used dry bushings	**10%**
Other	**4%**

Utilities are starting with the low-hanging operational measures, whereas hardening – which takes longer and is saddled with a longer path to cost recovery – comes later in the phased approach.

THREATS & CHALLENGES

What is the biggest challenge for your utility when it comes to physically securing your transmission substations?



- Path to cost recovery is not clear and/or is very difficult **43%**
- Grid security is not enough of a priority with upper management **19%**
- Government agencies do not provide enough direction or support **18%**
- Other **11%**
- Information-sharing between stakeholders is lacking **9%**

COST BARRIERS

When utility executives were asked about their greatest challenge for physically securing their substations, more than 40% cited barriers to cost recovery. This is particularly an issue for IOUs, with 65% citing an unclear path to cost recovery as a barrier. In comparison, less than 20% of respondents from other utilities cite cost recovery as a challenge.

The biggest challenge for utilities taking actions to improve physical grid security is an **uncertain or difficult path to cost recovery.**

Justifying the costs of physical security improvements may be problematic for regulated IOUs due to a number of reasons. Investments that are derived from regulatory requirements have a clearer path to cost recovery. Prior to the FERC directing NERC to develop CIP standards, there was no definitive regulatory requirement for physical grid security. The benefits of security measures are difficult to quantify because it involves evaluating a reduced risk of damages, or avoided cost from physical security incidents. In addition, expenditures must be approved at various levels – by utility management, FERC, and state utilities commissions.

VULNERABILITY ASSESSMENTS

Power grid infrastructure is vulnerable to numerous and diverse physical threats according to utilities. Threats include accidents, theft or vandalism, geomagnetic disturbances (solar activity), electromagnetic pulses (EMP), availability of sensitive information, natural disasters, and aging infrastructure. Despite the rarity of sabotage and shooting incidents, most utilities still considered them a minor to moderate threat, with only 20% saying they posed no threat.

While high-profile attacks such as the Metcalf shootings garner the bulk of media attention, they are not the most serious vulnerabilities according to utilities. Natural disasters and aging infrastructure pose the most significant threats to critical assets. Weather and natural hazards including severe winds, flooding, storm surges, forest fires, earthquakes and ice are regular threats faced by utilities. Compounding these vulnerabilities, aging power transformers are at increased risk of failure from such events.

Rank your potential transmission substation physical security vulnerabilities for damage and reliability impacts on a scale of 1-5 (1-no threat, 5-maximum threat).

	No threat	Minor threat	Threat	Critical Threat	Maximum Threat
Natural disasters (severe winds, flooding, storm surges, forest fire, earthquakes, or ice)	4%	32%	31%	25%	9%
Accidents, including those involving wildlife, automobiles, or utility workers	14%	47%	32%	6%	1%
Aging infrastructure prone to failure or destruction	7%	30%	39%	20%	4%
Theft or vandalism	10%	42%	28%	17%	4%
Shootings and planned sabotage	20%	41%	25%	8%	5%
Geomagnetic disturbances from solar activity	26%	44%	19%	6%	4%
Availability of sensitive information on critical assets	15%	34%	28%	19%	4%
Electromagnetic Pulse Disturbances (EMP)	18%	44%	20%	11%	6%

Long lead times and limited availability of spare parts and components hamper utilities' efforts to repair damaged transformers. Almost 40% of respondents have experienced issues with lead times or availability of parts for repair of HV transformers. Due to costs, most utilities cannot simply maintain significant spare part inventories. Issues related to the availability of qualified repair technicians were also cited as an issue by nearly one-quarter of respondents.

When a transformer is damaged beyond repair, replacement is complicated by lead times, costs, transportation and installation. Large power transformers typically have unique designs, making their replacement more difficult, with lead times between 12 and 24 months. Replacement transformers can range in cost from $2 million to $7.5 million, according to the Department of Energy. Transportation and installation further increase replacement costs. If a physical attack were to damage a critical HV transformer beyond repair, this substantial lead time could result in extended outages.

The majority of utilities surveyed have encountered problems with replacing HV transformers, with half of respondents citing long lead times. These large power transformers must be transported by special railcars or flatbed trucks designed to distribute their heavy weight, which can be 100 to 400 tons or more. Because of the limited availability of specialized transport, 20% of respondents have had challenges with getting replacement transformers delivered. Once on-site, a quarter of those surveyed have had structural issues in placing new transformers due to unique configuration, physical size or concrete pad integrity.

The replacement of large transformers is a difficult challenge for utilities, as lead times **typically range from 12 to 24 months.**

GRID SECURITY STRATEGIES & APPROACHES

AS UTILITIES HAVE NAVIGATED CIP-014 REQUIREMENTS, they have identified vulnerabilities of their HV substation assets. To address these vulnerabilities and minimize risks, utilities are planning additional operational and monitoring improvements. Nearly 50% of respondents are planning to deploy alarm systems that alert them when tampering or intrusion occurs. Additional hardware and software to limit access so that only authorized personnel are able to enter critical substations is planned by 56% of utilities respondents and 45% plan to install electronic monitoring and remote surveillance devices. The number of utilities that plan to use drones in the future will increase, but still represents a small percentage of utilities' monitoring measures.

The top three operational and monitoring measures utilities are planning to use to detect and deter security threats are limiting access to authorized personnel, deploying alarm systems, and utilizing remote surveillance.

While 40% of respondents indicated their utility has not undertaken any hardening actions in the last two years to deter and delay damage, 77% are planning to take steps. Planned hardening activities include: installing physical barriers (46%), managing visibility (44%) and strengthening communications (34%) are the most common measures planned. Other initiatives include installing redundant cooling systems, hardening

managing visibility (44%) and strengthening communications (34%) are the most common measures planned. Other initiatives include installing redundant cooling systems, hardening control houses, relocating equipment, and using ballistic shielding for transformers. Some utilities are planning on using dry bushings, which reduce the chances of collateral damage.

More than 80% of the utilities surveyed are taking steps to improve response and recovery from incidents at transmission substations, including increasing coordination with law enforcement agencies, engaging with other utilities to benchmark best practices, developing incident recovery plans and establishing rapid response teams. The high percentage of respondents that have plans to address recovery from incidents reflects an increasing awareness of the potential severity of physical attacks on the electric grid.

More than 80% of the utilities surveyed have already taken steps to improve response and recovery from incidents at transmission substations.

What design modifications and/or hardening actions is your utility planning to implement to deter/delay physical security threats at transmission substations in the future? (Select all that apply)

Installing physical barriers including fencing, perimeter walls, or locks	**46%**
Enhancing substation lighting, vegetation, or other measures to manage visibility of assets and detect threats	**44%**
Strengthening the resiliency of communications	**34%**
Reconfiguring location of assets at transmission stations to limit impact of a single event	**32%**
Hardening control houses	**24%**
No actions have been planned	**23%**
Relocating spare equipment to off-site storage areas	**23%**
Installing redundant cooling systems	**17%**
Using less flammable oil in substation equipment	**15%**
Armor or ballistic shielding of transformers and other HV equipment	**14%**
Use of dry bushings	**12%**
Camouflaging substation equipment through enclosure or placing assets underground	**7%**
Other	**3%**

A CRITICAL NEED

Utility executives cite a number of challenges for enhancing physical grid security, but perhaps the biggest obstacle is in recovery. The crucial role that large power transformers play in maintaining grid reliability, their vulnerability to attack and damage, and the difficulties in replacing them presents utilities with a significant problem. Given the long lead times for HV transformer replacement parts and components, a large number of utilities are stockpiling spare equipment, either at substations or at off-site locations or maintaining incremental spares. However, as discussed earlier, cost can be a barrier to having enough spare components on hand in case of emergencies. As a result, some utilities are leveraging collaborative industry programs to address this problem.

The Edison Electric Institute runs the federally-approved Spare Transformer Equipment Program (STEP) for coordinating a rapid recovery in the event of an intentional physical attack. Each of the 54 participating utilities maintains a specific number of spare transformers and sells its equipment to other utilities in the event of a triggering emergency event. Another program recently announced by eight utilities is Grid Assurance, which aims to improve the resiliency from physical attacks by pooling assets and pre-planning logistics to speed recovery. Under the program, Grid Assurance would own and maintain the spare equipment so that in the event of physical attack, repair and replacement would be deployed more efficiently in less time. Almost a quarter of survey respondents are participating in a shared equipment program such as STEP or Grid Assurance.

How is your utility addressing vulnerabilities related to repair or replacement of critical transformer equipment? (Select all that apply)

Stockpile spare equipment at off-site centralized location(s)	**42%**
Utilize NERC's Spare Equipment Database as needed	28%
Developing a modular rapid recovery transformer standard	26%
Maintain incremental spares above normal level	23%
Participate in a shared transformer stockpile/reserve program	23%
Stockpile spare equipment at substations	22%
No actions have been taken	21%

The ability to rapidly repair or replace high-voltage transformers in the event of an emergency is a primary concern for many utilities. The overwhelming majority of respondents feel that establishing a national Strategic Transformer Reserve program is important or critical.

Another tool for equipment sharing is NERC's Spare Equipment Database, in which utilities voluntarily provide data on their spares. The use of the database is meant to facilitate transformer sharing and mutual assistance agreements in the event of a major grid event. This database is being used by 28% of respondents to prepare for emergencies.

Beyond these initiatives, The U.S. Department of Homeland Security, the Electric Power Research Institute (EPRI), CenterPoint Energy and ABB have partnered to create a prototype modular rapid recovery transformer, called "RecX." The goal of creating a rapid response HV transformer is to improve the interoperability with other large power transformers, rather than relying on matching components. While large utilities have mobile transformers, they are typically low-voltage transformers used on the distribution side. Very few utilities have spare HV transformers. The plug-and-play modular HV transformer is intended to be a temporary replacement that allows power to be restored more quickly while a permanent transformer is procured. This effort has the support of 26% respondents who are working to develop a modular rapid recovery transformer standard.

Reflecting the critical need for rapid recovery from physical grid attacks, the overwhelming majority of respondents (74%) feel that establishing a national Strategic Transformer Reserve program is important or critical. The idea behind this program is to strategically place reserve large power transformers around the country to complement existing industry collaborative programs. The idea of such a nationwide strategy has captured the attention of congressional leaders who have introduced legislation to authorize such a program.

Looking across the various spare equipment sharing programs, it is clear that utilities recognize that replacement of large power transformers is perhaps the most important issue related to physical grid security.

LOOKING AHEAD

As utilities progress further in their CIP-014 initiatives, **their ability to address vulnerabilities and protect critical assets will improve.**

Protecting the electric grid from physical security threats requires assessment, planning and undertaking a number of actions to detect, deter and ultimately recover from attacks. A number of NERC CIP-014 deadlines are fast approaching. By October 1, 2015, utilities must have completed their initial risk assessment for identifying critical facilities. By May 5, 2016 they must complete a threat and vulnerability assessment. As utilities progress further in their CIP-014 initiatives, their ability to address vulnerabilities and protect critical assets will improve.

Because the reliability of the electric grid is dependent on a small number of high voltage transformers at critical substations, the ability to protect and rapidly repair or replace these assets in the event of an emergency is a primary concern of many utilities. The majority of utility executives support a coordinated industry approach, whether through an existing spare transformer exchange program, the creation of a national Strategic Transformer Reserve program or the development of a modular, rapid recovery large power transformer.

Rapid response and recovery from incidents is a priority for utilities, reflecting the reality that despite preventive measures to detect and deter threats, some emergencies will inevitably occur. When that happens, resiliency – and the ability to quickly restore power – will be critical.