Written Testimony

Hearing of the Senate Committee on Energy and Natural Resources
Subcommittee on Energy

United States Senate

Mr. Robin Manning
Vice President, Transmission
Electric Power Research Institute

"Hearing to receive testimony on S. 3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions"

July 12, 2016

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers, as well as experts from academia and industry, to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries.

The subject of today's testimony is the impact on the power industry of potential cyber and physical security activities, including high-impact, low-frequency (HILF) events. Although EPRI recognizes the introduction of S. 3018, today's testimony addresses the technical aspects of these events, rather than any proposed legislation. HILF events include severe weather and other natural events; cyber, physical, or coordinated attacks; pandemics; unanticipated severe shortages of fuel or water for power generation; and electromagnetic pulse (EMP) and intentional EM interference (IEMI) attacks. There are inherent vulnerabilities in the transmission grid system to these threats because the severity is generally greater than the design basis for the system. To eliminate these vulnerabilities would be cost prohibitive and would thwart the objective to provide reliable, safe, environmentally responsible, *and* affordable power.

A prudent approach is to assess the vulnerabilities, understand the impacts should these types of events occur, and develop cost-effective countermeasures to reduce the risk by increasing system resiliency. In the context of the transmission system, resiliency is the ability to harden the system against—and quickly recover from—HILF events, which include both severe weather (including space weather), and man-made attacks. HILF events can disrupt generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines, other fuel transport channels, and telecommunications. There are a large number of possible mitigating technologies from which to choose to enhance transmission resiliency in the face of potential HILF events.

My testimony today focuses on the security considerations of HILF events, specifically: 1) the threat of HILF events to the grid including EMP, geomagnetic disturbance, and IEMI; 2) risk management approaches to address EMP threats; 3) EPRI's recently-launched EMP research program; 4) the threat of cyber security to the grid; and 5) risk management approaches to address cyber security. Physical

security can also be considered a HILF threat; however, the topic of physical security is quite broad and as such will be considered outside the scope of today's brief remarks. All remarks are based upon EPRI research as well as industry knowledge and documents available in the public domain.

Electromagnetic Pulse

Electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) are often discussed together when evaluating potential impacts on the power system and approaches for improving system resiliency. While these events are both considered HILF events (along with physical attacks, severe storms, earthquakes, and other events), there are very important differences between EMP and GMD events that should be understood when evaluating resiliency improvement priorities and investment decisions.

- EMP refers to a very intense pulse of electromagnetic energy, typically caused by detonation of a nuclear or other high-energy explosive device. High-altitude EMP (HEMP) is a nuclear warhead detonated hundreds of kilometers above the Earth's surface to produce more widespread effects (areas affected can be hundreds of kilometers in diameter). It is generally accepted that a HEMP will require a high-altitude delivery device (e.g., a missile) which will require a high level of sophistication and logistics. As a result, the HEMP threat is most often associated with potential attacks from nation-states.

- EMP events are intentional, man-made attacks of electromagnetic energy specifically for the purpose of disrupting and/or damaging electrical/electronic systems. The three categories of EMP may have different impacts on transmission systems (see figure 1).

    - E1—Very fast rise time, may result in damage to electronic components either directly, or indirectly by coupling into the attached wires. GMD events do not have this characteristic.
    - E2—Characteristics are similar to lightning and consequently can result in damage to electronics and potential flashover of distribution class insulation. Neither GMD nor IEMI have this characteristic.
    - E3—Characterized by a longer duration and low-frequency content similar to GMD but much shorter in duration. EMP has two potential grid impacts resulting from the flow of geomagnetically-induced currents (GICs): 1) voltage collapse due to increased reactive power consumption and misoperation of protection systems due to harmonics, and 2) additional hotspot heating in transformers.

- EMPs can occur with little or no warning. With the possible exception of enhanced visibility tools, most operational strategies are inapplicable. Therefore, response to the EMP threat generally comes in the form of hardening assets ahead of time to reduce initial damage, reducing the duration of the interruption, and providing workable routes to recovery.

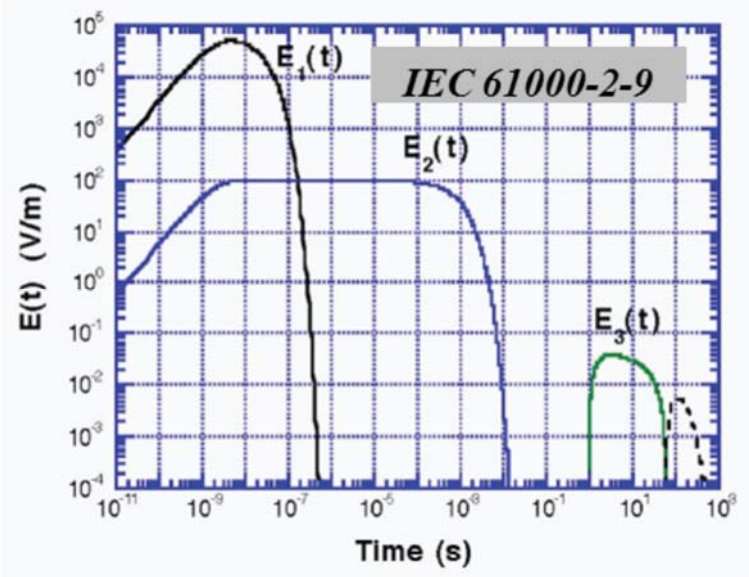


Figure 1. EMP Characteristics: Electric field magnitude as a function of time for an EMP pulse.

Geomagnetic Disturbance

- Geomagnetic disturbances (GMDs) are natural phenomena which induce slowly changing, quasi-direct currents onto the power grid. These currents are similar to those created in an E3 EMP event; however, the duration of the E3 pulse is much shorter than a GMD.

- Locations that are closer to the Earth's poles are more susceptible to GMDs than lower latitudes. Space weather warning systems provide estimates of GMD activity as much as four days before the storm reaches Earth. These systems use direct observations of the sun. Accuracy of the forecast improves when the storm reaches NOAA's DSCOVR satellite, about one hour before the storm reaches the Earth. DSCOVR is an Earth observation and space weather satellite launched on February 11, 2015. It is positioned at the Sun-Earth L_1 Lagrangian point, 930,000 miles from Earth, to monitor solar wind conditions; provide early warning of approaching corona mass ejections; and observe phenomena on Earth including changes in ozone, aerosols, dust and volcanic ash, cloud height, vegetation cover, and climate.

- Monitoring systems have been installed in multiple locations which measure the GIC currents in transformers across the grid.

- GMD events, many of which are low magnitude, occur on a regular basis, which enable grid operators to improve their understanding of the phenomena, determine the impacts on the grid, and evaluate trial countermeasures. These storms can provide an indication of the grid's response to severe storms, and support development of prudent operational strategies.

- The inherent nature of GMD phenomena do not threaten ground-based grid electrical components. Large equipment heating and voltage stability are the primary challenges.

- Although severe storms can occur any time during the approximately eleven-year solar cycle, more storms occur during the peak of the solar cycle.

- GMD storm duration can be in the order of hours or days, while the duration of EMP is considered to be in the order of minutes.

- Utilities have established operational strategies to mitigate risk during GMD events. NERC has two compliance requirements in place or in approval; EOP-010-1 and TPL-007-1. EOP-010-1 is in place and requires utilities to have operational procedures to mitigate the effects of GMD events, while TPL-007-1, is waiting FERC approval and would require utilities to: 1) perform vulnerability assessments of their systems to determine the potential impacts of a 1-in-100-year GMD event, and 2) develop mitigation measures if performance criteria are not met.

Intentional Electromagnetic Interference

Like EMP, intentional electromagnetic interference (IEMI) generates and delivers electromagnetic energy. IEMI is generated and delivered locally, and employs no nuclear material. IEMI devices have the potential to impact electronic assets in nearby locations such as control centers. Critical electronic equipment in these locations include relays, supervisory communications and data acquisition (SCADA) systems, communication networks, and energy management systems (EMS).

Individual grid components are inherently vulnerable to these threats because the severity is generally greater than the design basis for the system. Today's power systems are operating in an increasingly complex electromagnetic environment in which large current and voltage components, sensitive electronics, digital signals, and analog waveforms coexist and interact. The widespread proliferation of smart grid systems, including substation automation and syncrophasor systems, are part of this increasing complexity. However, extensive grid-wide damage by IEMI would require a tremendous coordinated effort as the loss of individual components do not, in and of themselves, cause cascading loss of the grid. NERC CIP-014 would require utilities to protect their system against that risk and develop mitigation strategies if they do not meet the specified performance criteria.

Risk Management Approaches to Address EMP Threats

EPRI is working with industry stakeholders to characterize EMP threats, including HEMP attack, EMP, and local IEMI attack. This work is providing the design basis for assessing vulnerability and developing mitigation strategies. EPRI is gathering available data on component vulnerabilities to the benchmark threats. The results, when complete for all critical components, will support calculation of the system impact. EPRI is gathering leading practices by electricity providers who have applied trial implementation of countermeasures to reduce vulnerability.

A number of risk-management approaches can be considered to reduce the impact of EMP on the transmission system. Some of these methods are being considered by various utilities for implementation:

Risk Assessment
Prudent application of scarce resources requires careful countermeasure and site selection procedures. While it may be difficult to identify regions of the grid that are more likely to be attacked by an EMP, it may be possible and prudent to identify and focus resources on the most critical components necessary for the reliable operation of the transmission system.

Hardening of Assets

Hardening for new and existing systems generally focuses on reducing the impact of electromagnetic waves on electronic equipment. Some hardening options include:

- New control rooms with EM shielding in the form of a Faraday cage are being implemented at some locations. External cable entrances must be considered, including the number and location of penetrations as well as the implementation of surge protection, filtering, and grounding strategies. Other challenges include staff entrances/exits and ventilation ducts.

- New relay houses that are EMP-hardened are being developed and tested by some utilities. These relay houses use metal buildings with special consideration given to ensure bonding of metal members, improved grounding, and cable entrances.

- The use of power supply and communication cables with integrated shields, as well as consideration for the grounding strategies for these shields, is being implemented (e.g., individually-shielded, twisted pair cables with an overall shield that is grounded).

- Surge protection and grounding of cables entering and exiting the facilities is routine practice due to everyday lightning activity that could affect the electronic equipment.

- Interference filtering can be applied at cable entry points to reduce high-frequency conducted energy that can impact the attached electronic activity.

- Relocation of unprotected, sensitive control equipment to inside the shielded enclosures.

- Relocation of control cables to a lower EM environment, such as conductive conduit, to reduce induced voltage.

- Increase the use of fiber-optic cables rather than metallic cables for communications. Fiber-optic cables have much lower susceptibility to EM impacts.

- Utilities are engaging original equipment manufacturers (OEMs) to incorporate EM resiliency into new components, such as relays and communications systems.

- Neutral blockers for transformers to reduce the impact of GMD are being evaluated. These blockers may aid in the reduction of induced E3 currents. The impact of neutral blockers on system operation requires consideration.

Recovery Options

- Consider spare parts. Because a severe EMP attack can damage key electronic system components, strategic stockpiling is prudent. Sparing can be considered for relays, which are susceptible to the E1 and E2 component of an EMP. Storing critical spares in shielded EM enclosures is a consideration.

- Other equipment that supports restoration could also be protected from EMP. This includes equipment associated with black start, backup communications systems, transportation, and

diagnostics components.

- Asset owners may consider adding the EMP threat to their transformer spare parts strategy. Lower voltage transformers below 69 kV can be affected by the E1 and possible E2 portions of an EMP if they are not protected with surge arresters. Larger power transformers are unlikely to be impacted directly by E1 or E2.

- In addition to spares, mobile systems to support recovery can be considered, such as mobile transmission capacitor banks, mobile substations (typically for distribution), and mobile substation control houses.

- Redundant systems that are not susceptible to EMP, such as electromechanical relays, can be applied.

- Utilities may consider disconnecting, and possibly grounding, redundant relays and communication systems, so that they are available after an EMP. However, caution is warranted for this approach because system resiliency to traditional threats may be compromised.

- Restoration plans and training can be embellished to incorporate recovery from EMP. Relay technicians will be especially important to EMP recovery.

EPRI's EMP Research Project

Electromagnetic pulse events are a growing concern in the energy business. While the industry has worked to develop effective responses to GMD, little definitive work has centered on the effects of an EMP attack.

Numerous constituencies are pressing to ensure the electric power system is more resilient to a large EMP event, but technical information is inconsistent and options to increase resilience through hardening and recovery are not well-defined. Some proposed approaches are high-cost and lack the technical basis to substantiate their viability.

EPRI is collaborating with the U.S. Department of Energy to develop objective options to respond to the EMP threat. EPRI's EMP research project intends to provide a sound, technical basis by which utilities can effectively evaluate potential impacts, mitigation, and recovery plans.

EPRI's three-year, collaborative research effort aims to characterize specific EMP threats, assess substation component vulnerability, assess methodologies for determining system impact, and assess or develop mitigation strategies—including hardening and recovery—to enable utilities to make important decisions about system resiliency.

Cyber Security

With the increased use of digital devices and more advanced communications and other information technology (IT), the overall attack surface has increased. For example, substations are modernized with new equipment that is digital, rather than analog. These new devices include commercially available operating systems, protocols, and applications as an alternative to proprietary solutions that are specific

to the electric sector. Many of the commercially available solutions have known vulnerabilities that could be exploited when the solutions are installed in operational technology (OT) system components. Potential impacts from a cyber event include: billing errors, brownouts/blackouts, personal injury or loss of life, operational strain during a disaster recovery situation, or physical damage to power equipment.

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways (e.g., two-way communications and wired and wireless communications) than in the past. These new components will operate in conjunction with legacy equipment that may be several decades old, and which provide no cyber security controls. Traditional IT devices typically have a life span of three to five years. In contrast, OT devices can have a life span of up to 40 years or longer. With the constantly changing IT and threat environments, addressing potential cyber security events is a challenge.

Another change is the convergence of IT and OT. Historically IT has included computer systems, applications, communications technology, and software to store, retrieve, transmit, and process data typically for a business or enterprise. OT has historically focused on physical equipment-oriented technology that is commonly used to operate the energy sector. Multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (i.e., situational awareness) and events (both unintentional, such as a component failure, and malicious) that may impact an organization's security posture, and responses to those events.

Cyber Security Risk Management

Cyber security is a priority for critical infrastructures, especially electric utilities. To adequately address cyber security risks, utilities must identify basic differences between the security requirements for IT systems and the security requirements for OT systems. In general, the focus for IT systems is confidentiality of information; for example, customer energy use and privacy information. The focus for OT systems is availability and integrity, to ensure that the reliability of the grid is maintained even in the event of a cyber security incident. The OT systems also have performance requirements, and any significant delay in sending and/or receiving data and commands could adversely impact the reliability of the grid. Typical IT security controls, such as cryptography and vulnerability scanning, that have been implemented in OT systems could cause systems to fail. Because of these differences, utilities need to take care so that implemented security controls do not adversely impact the reliability of the grid.

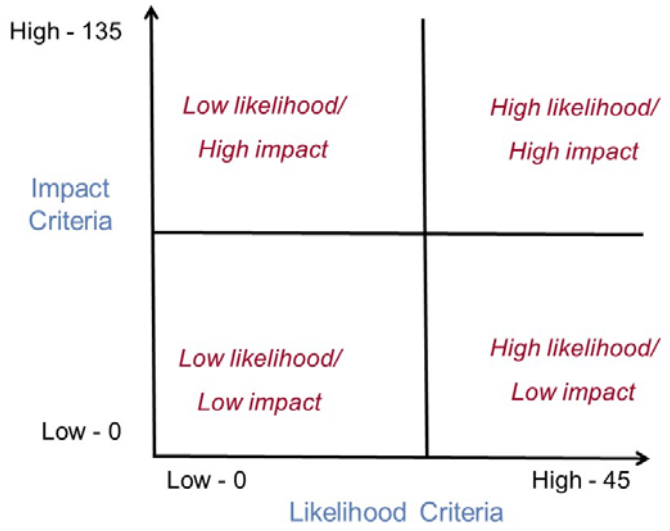
- To adequately address potential threat agents and vulnerabilities, cyber security should be included in all phases of the system development life cycle—from the design phase through implementation, operations and maintenance, and sunset. Cyber security should address deliberate attacks launched by disgruntled employees and nation-states, as well as non-malicious cyber security events (e.g., user errors, incorrect documentation, etc.). Currently, the majority of cyber security events are non-malicious.

- Cyber security must be prioritized with the other components of enterprise risk because organizations, including utilities, do not have unlimited resources, personnel, and funds. *Risk* is the potential for an unwanted impact resulting from an event. *Enterprise risk* addresses many types of risk such as investment, budgetary, program management, legal liability, safety, and inventory risk, in addition to cyber security. A cyber security risk management strategy should be a component within an organization's enterprise risk management strategy.

- Risk assessment is a key planning tool for implementation of an effective cyber security program and involves identifying threats, vulnerabilities, and the potential impact and risk associated with the exploitation of those vulnerabilities. Risk assessments are performed on systems. Once the risk is determined, the organization needs to determine a course of action: accept, avoid, mitigate, share, or transfer.

- Organizations should perform risk assessments on an ongoing basis throughout the system life cycle. The two criteria used in a risk assessment are impact and likelihood. EPRI, in conjunction with utilities, academia, researchers, and vendors, developed a risk assessment methodology that is based on a typical IT methodology with impact and likelihood criteria that are specific to the electric sector. This work was performed as part of the National Electric Sector Cybersecurity Organization Resource (NESCOR) project—a U.S. DOE funded public-private partnership.

    - Some of the NESCOR impact criteria include: system scale, safety concern, ecological concern, restoration cost, negative impact on generation capacity, and negative impact on the bulk transmission system.
    - Some of the NESCOR likelihood criteria include: skill required, accessibility (physical), accessibility (logical), and attack vector. A score of 0, 1, 3, or 9 is determined for each criterion, then a sum is calculated for impact and likelihood.
    - The resulting score can be displayed on a graph, as shown below. The systems that fall in the upper right quadrant, high likelihood/high impact, are the highest priority for the organization as are the mitigation strategies for these systems.



Cyber Security Mitigation Strategies

Utilities, government agencies, academia, research organizations, and vendors are collaborating on many projects to develop tools and techniques to address cyber security threats and vulnerabilities. This collaboration is important to ensure that the unique cyber security requirements of the electric sector are addressed.

Several requirements documents that specifically address the electric sector provide mitigation strategies. Three of these documents are highlighted below.

- The first document is the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, initially published in 2010. The development was led by NIST with a team of volunteers from the private sector, academia, research organizations, and government. Roughly 150 individuals volunteered their time to author this document. This is the first document that focused on the electric sector, and it has been distributed and used worldwide.

- A second document is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which guides electric utilities and grid operators in assessing their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. The maturity model was developed as part of a White House initiative led by DOE in partnership with the Department of Homeland Security (DHS) and involved close collaboration with industry, other federal agencies, and other stakeholders. This document is also used worldwide.

- The third document is a joint publication of DOE and EPRI, "Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology." The purpose of the report is to specify a risk assessment process that may be used by utilities. Included are high-level diagrams that illustrate the risk assessment process at the security requirements and security-control-selection stages, as well as for ongoing assessment and for assessing emerging changes. A second objective is to illustrate how to use the content of the NESCOR cyber security failure scenarios and impact analyses document in the risk assessment process.

DOE has been the designated Sector-Specific Agency (SSA) for the energy sector since 2003, and research and development has been identified in the Sector-Specific Plan (SSP) as a key source of innovation and productivity for the energy sector. Since more than 80 percent of the country's energy infrastructure is owned by the private sector, DOE has initiated several collaborative research efforts. Two are highlighted below:

- A key mission of DOE's Office of Electricity Delivery and Energy Reliability (OE) is to enhance the reliability and resilience of the nation's energy infrastructure. Cyber security of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE designed the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cyber security solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cyber security capabilities for energy delivery systems.

- DOE published a *Roadmap to Achieve Energy Delivery Systems Cybersecurity* in 2011 that provides a plan to improve the cyber security of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for

energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade.

The vision within the roadmap states: *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.* The roadmap is an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*. The 2011 roadmap addresses gaps created by the changing energy sector landscape and advancing threat capabilities, and emphasizes a culture of security.

Many utilities and EPRI map their R&D programs to the strategies defined in the *Roadmap* and to the domains specified in the ES-C2M2. These common categories are used by utilities, academia, and research organizations in the public and private sectors as they define and prioritize their research agendas. This is particularly important with the constantly changing threat environment.

Another NESCOR project focused on the development of *failure scenarios* for the electric sector. A *cyber security failure scenario* is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Each scenario includes a title, short description, relevant vulnerabilities, impact, and potential mitigations. Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality
- Failures due to data integrity attacks
- Communications failures
- Human error
- Interference with the equipment lifecycle
- Natural disasters that impact cyber security posture

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence.

Included below is a sample failure scenario.

AMI.26 Advanced Metering Infrastructure (AMI) Prepaid Billing Cards are Compromised Resulting in Loss of Revenue

Description: The prepaid billing cards for AMI are compromised. Example compromises include tampering with cards to change the credit amount, erasing the logic that decrements the credit amount remaining, or forging cards.

Relevant Vulnerabilities:

- *System assumes data inputs and resulting calculations are accurate* on prepaid billing cards inserted into a meter.
- *System permits unauthorized changes* to AMI billing information on prepaid billing cards.

Impact:
Loss of revenue

Potential Mitigations:

- *Design for security* in the payment system.
- *Check software file integrity* (digital signatures or keyed hashes) on the prepaid billing card contents.
- *Authenticate data source* (i.e., prepaid billing cards) for AMI billing.
- *Perform security testing* as a part of system acceptance testing.

For utilities that do not have readily available cyber security staff, the failure scenarios may be used as part of the overall risk management process to begin addressing potential cyber security events. For all utilities, the failure scenarios may be used to train new personnel and for refresher training for all staff. Finally, the failure scenarios may be used as input to tabletop exercises. Tabletop exercises are discussion-based sessions where team members meet in an informal classroom setting to discuss their roles during an emergency and their responses to a particular situation. Many tabletop exercises can be conducted in a few hours.

The NESCOR failure scenarios have been used by researchers and utilities around the world.

Conclusion

Potential impacts of cyber security, EMP, GMD, and IEMIs on existing and new power grid infrastructure requires concrete, scientific evaluation and analysis. Threats must be quantified and addressed to allow for common sense and robust mitigation strategies. While we've identified several strategies in today's testimony, much more research and information is needed, especially as technology advances and as new cyber security threats enter into the equation.

EPRI will continue to offer technical leadership and support to the electricity sector, public policy-makers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity.