U.S. Department of Energy
Washington, DC 20585

Date: **April 2, 2014**

To: **Members of the Public**

From: **Quadrennial Energy Review Task Force Secretariat and Energy Policy and Systems Analysis Staff, U. S. Department of Energy**

Re: **Public Meeting on "Enhancing Resilience in Energy Infrastructure and Addressing Vulnerabilities"**

Introduction

On Friday, April 11, 2014, at 10 a.m. in room HVC-215 of the U.S. Capitol, the Department of Energy (DOE), acting as the Secretariat for the Quadrennial Energy Review Task Force, will hold a public meeting to discuss and receive comments on issues related to the Quadrennial Energy Review (QER). The meeting will focus on infrastructure vulnerabilities related to the electricity, natural gas and petroleum transmission, storage and distribution systems (TS&D). The meeting will consist of two facilitated panels of experts on identifying and addressing vulnerabilities within the nation's energy TS&D infrastructure. Following the panels, an opportunity will be provided for public comment via an open microphone session.

1. The Quadrennial Energy Review

On January 9, 2014, President Obama issued a Presidential Memorandum: Establishing a Quadrennial Energy Review. The Memorandum established a Quadrennial Energy Review Task Force to be co-chaired by the Director of the Office of Science and Technology Policy and the Director of the Domestic Policy Council. The Secretary of Energy was directed to provide support to the Task Force, including support for coordination activities related to the preparation of the QER report, policy analysis and modeling, and stakeholder engagement.

The initial focus for the QER will be our Nation's infrastructure for transporting, transmitting, storing and delivering energy.

As America's energy sector continues to expand and evolve, so will the challenges and opportunities associated with supporting new sources of energy. Many of these challenges result from changes that can fundamentally improve America's energy security, economic competitiveness and help achieve long-range environmental goals. Technologies such as shale gas, tight oil, electric vehicles, solar PV, wind

power and LED lighting are on track to transform our economy for the better.[1] In just the past five years, the cost of solar photovoltaic panels has dropped by more than 75 percent.[2]

Strategically deployed, these resources have the potential to clean up the air in our cities, reduce America's vulnerability to unstable international oil markets and help build an economy that is more competitive and more efficient.

Today, America has a commanding advantage in energy prices compared to many of its global peers and competitors. In 2013, U.S. industrial electricity prices were among the lowest in the Organisation for Economic Co-operation and Development (OECD). These prices actually fell between 2008 and 2012 (see Table 1). American industries paid about $66 per megawatt hour of electricity in 2012, whereas German, Japanese and French industrial users paid $148/MWh, $194/MWh and $116/MWh respectively.

Table 1. Comparison of OECD Industrial Electricity Prices

	2008	2012
USA	$68/MWh	$66/MWh
Germany	$130/MWh	$148/MWh
Japan	$115/MWh	$194/MWh
France	$104/MWh	$116/MWh

Source: OECD Electricity Statistics 2013

These differences are material and a major reason that multi-national companies are increasing manufacturing and petrochemicals investments the United States. At the same time, U.S. CO_2 emissions have declined by about 10 percent since 2005. One major driver for these trends is increased utilization of natural gas, but renewables, electric vehicles and higher fuel economy were also instrumental in reducing CO_2 emissions.[3]

To propel these positive trends forward and ensure that America can take full advantage of this favorable energy landscape, it will be critical to safeguard and improve the infrastructure that undergirds America's energy system. Elements of our current infrastructure are challenged by transformations in energy supply, markets, and patterns of end use; issues of aging and capacity; impacts of climate change; and cyber and physical threats. Any vulnerability in this infrastructure may be exacerbated by the increasing interdependencies of energy systems with water, telecommunications, transportation, and emergency service systems. Modernized infrastructure can spur economic growth, attract new businesses, enable the

---

[1] IHS. 2013. *America's New Energy Future: The Unconventional Oil & Gas Revolution and the U.S. Economy, Volume 3*. IHS. Available at: http://www.energyxxi.org/sites/default/files/pdf/Americas_New_Energy_Future_ Phase3.pdf (accessed April 1, 2014)

[2] U.S. Department of Energy (DOE). 2013. *Revolution Now: The Future Arrives for Four Clean Energy Technologies*. DOE. Available at: http://energy.gov/sites/prod/files/2013/09/f2/Revolution%20Now%20--%20The%20Future%20Arrives%20for%20Four%20Clean%20Energy%20Technologies.pdf (accessed April 1, 2014)

[3] Energy Information Association (EIA). "AEO2014 Early Release Overview," (December 16, 2013). EIA. Available at: http://www.eia.gov/forecasts/aeo/er/tables_ref.cfm (accessed April 3, 2014)

development of business models and industries that are dependent on these underlying public goods, and facilitate the transformation to a cleaner, low-carbon economy.

The first Quadrennial Energy Review Report will serve as a roadmap to help address these challenges and opportunities of our evolving energy system.

2. Infrastructure Vulnerabilities

The National Infrastructure Protection Plan (NIPP 2013) defines vulnerability as "A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard."[4]

The consequences of various vulnerabilities can be assessed through the following areas of impact:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries)
- **Economic Impact:** Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage)
- **Psychological Impact:** Effect on the mental or emotional state of individuals and on public morale and confidence in national economic and political institutions
- **Mission Impact:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions[5]

Presidential Policy Directive 21 sets forth national policy on critical infrastructure security and resilience and directs the federal government to work with owners and operators and state and local governments to manage risks to critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. The goal of these efforts is to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.[6]

The QER will take into account previous analytical work on vulnerabilities of the United States energy infrastructure as well as comments from industry, government and academia and private citizens. The public comments at the Capitol Visitor Center will inform the QER Task Force efforts to outline specific sets and types of vulnerabilities and to define potential solutions to these vulnerabilities.

---

[4] U.S. Department of Homeland Security (DHS). 2013. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. DHS. Available at: http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience (accessed April 1, 2014).

[5] U.S. Department of Homeland Security (DHS), 2010. *DHS Risk Lexicon: 2010 Edition.* DHS. Available at: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (accessed April 1, 2014)

[6] The White House. Presidential Policy Directive 21 (PPD–21): "Critical Infrastructure Security and Resilience." February 12, 2013. Available at: https://fas.org/irp/offdocs/ppd/ppd-21.pdf (accessed April 1, 2014)

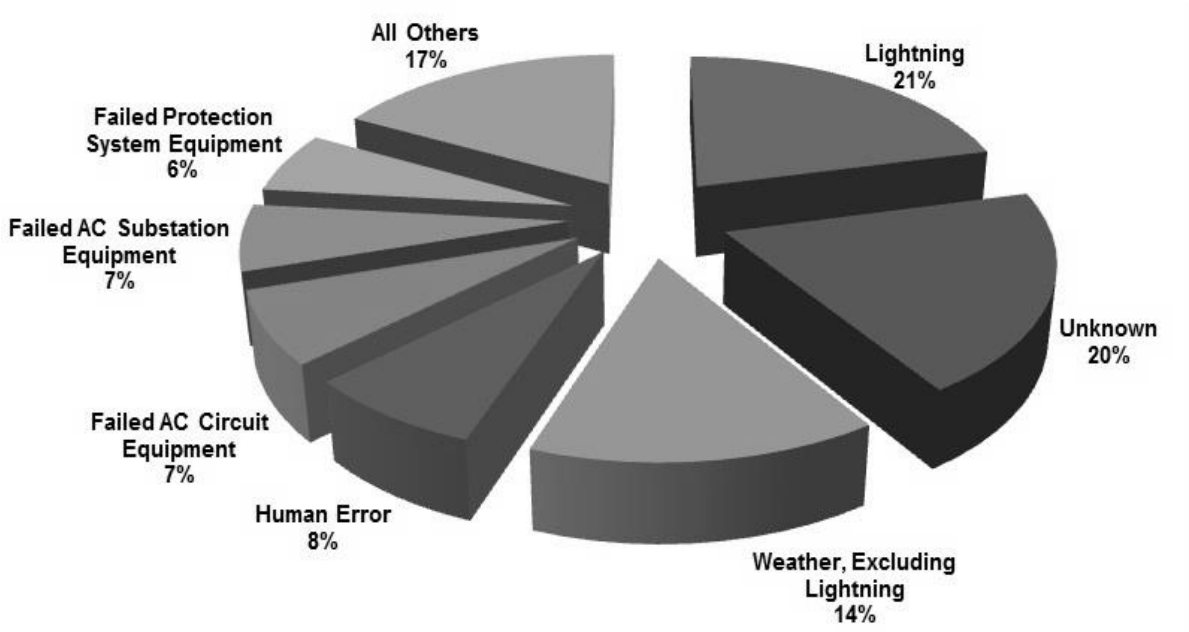

Figure 1. Transmission Outage Events by Cause from 2008 to 2012

From 2008–2012 weather-related outages accounted for the largest proportion of electricity supply disruptions.
Source: NERC SOR 2013, May 2013.

3. Types of Vulnerabilities

To catalogue the energy sector's disparate vulnerabilities it is necessary to consider a wide range of industries, fuel types, geographies, markets, technologies and timelines in the policy planning process. To simplify, we suggest categorizing vulnerabilities into three primary types:

1. **Systemically weak:** Somehow unstable, inflexible, or fragile and therefore vulnerable to possible operational failures that reduce its functionality or damage other portions of the economy
2. **Vulnerable to attack:** Can be compromised physically or operationally (destroyed, damaged or impaired) by a malicious actor
3. **Vulnerable to extreme events:** Not sufficiently resilient to withstand or recover from extraordinary conditions not associated with an attack (e.g. a flood, storm, earthquake, naturally-occurring electromagnetic pulse)

A basic explanation of these tiers of vulnerability follows.

Systemically weak

In theory, systems should be designed so that they will perform adequately under operating conditions that can be reasonably expected to occur. A wide variety of environmental and technical considerations must be taken into account to assure proper functionality of diverse energy systems. These range from air and water temperature; to congestion within various systems for transporting electricity, gas and liquid fuels; to market conditions.

Robustness to various weather-related events is an important consideration (see Figure 1). For instance, the grid should not go down in the face of a severe wind gust or snow storm that falls within the parameters that can be reasonably expected within a particular service area. One typical metric for this kind of preparation is that a facility or system is designed to withstand an extreme event with a probable reoccurrence over some interval of time (e.g., hundred year storm). In the electrical sector, another metric is (N-1) redundancy (e.g., a system should remain functional if 1 out of N components is destroyed or damaged). Nuclear reactors are designed to withstand "design basis threats" and "design basis accidents" based on probabilistic scenarios developed by the industry and licensing bodies.

In recent years major energy crises have been triggered by events that fall well within the range of normal operations for U.S. energy systems—which points toward the importance of such systemic weaknesses. For instance, the 2003 Northeast blackout was the result of a power system that was not adequately maintained (trees were not trimmed and control room operations were not correctly managed). Although the system was operating near peak capacity because of hot weather, such conditions were not unusual. When sagging electrical lines touched untrimmed tree branches, this resulted in a series of cascading failures that should have been manageable. Because of critical mistakes they instead resulted in electrical outages in large swaths of the eastern United States and Canada.[7]

Another example of a systemic weakness is the California electricity crisis of 2000–2001. During this time, California suffered a rolling electricity crisis largely due to a poorly designed regulatory scheme that was vulnerable to manipulation by energy traders.

Vulnerable to attack

Many parts of our energy system were not built with a fortress mentality and therefore may be vulnerable to attack. These attacks can be physical, information technology-based, or both.

- **Cyber-threats** to energy systems are growing and evolving. In 2013, there were 151 cyber incidents involving the energy sector that were reported to the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT). This was more than half of all incidents reported to the ICS-CERT in 2013 and was a significant increase compared to previous years. Reporting to ICS-CERT is voluntary and, therefore, these numbers may be a fraction of actual cyber incidents impacting the energy sector.[8] In some cases, cyber incidents involve the theft of technical, operational, personal, or otherwise restricted or proprietary data from public or private institutions. In other cases, cyber-attacks can be operationally or physically destructive. For example, in 2012 a cyber-attack on Saudi Aramco rendered 30,000 computers inoperable.[9]

---

[7] U.S.-Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.* Available at https://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf (accessed April 1, 2014)

[8] U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center. 2013. *ICS-CERT Year in Review—Industrial Control Systems Cyber Emergency Response Team.* U.S. Department of Homeland Security. Available at: https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf (accessed April 1, 2014)

[9] Reuters. "Aramco Says Cyberattack Was Aimed at Production." December 9, 2012. Available at: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0 (accessed April 1, 2014)

- **Kinetic attacks** are physical threats to energy infrastructure. These may be designed to produce localized or larger scale power or fuel outages, or wider destruction. One recent attempt to attack an electricity substation in Metcalf, California involved infiltration and targeting of transformers with firearms.[10]

Vulnerable to extreme events

Finally, the energy system is vulnerable to extreme events—some predictable and others so-called "black swan" events. The dividing line between these two kinds of extreme events is sometimes fuzzy. For instance, Hurricane Sandy and the Fukushima nuclear disaster were both extraordinary events for which the East Coast and Japanese energy systems were not adequately prepared. Some would argue that these events could have been predicted and prepared for.[11] Others argue that they were "black swan" events that resulted from a confluence of complex and unforeseeable factors.

In the case of Hurricane Sandy, a massive northerly hurricane and sea-level rise contributed to the devastating storm surge that destroyed many communities along the U.S. East Coast and damaged major energy ports and cities.[12] In the case of Fukushima, an earthquake and accompanying tsunami that were significantly larger than anything experienced in recent centuries overwhelmed inadequate defenses.[13] Both of these events were historically destructive, but some argue that they could and should have been anticipated and planned for.

Electromagnetic pulses and geomagnetic disturbances are additional examples of potentially high impact events that could impact the electricity grid (the Federal Energy Regulatory Commission has released two Notices of Proposed Rulemaking requiring the North American Electric Reliability Corporation to develop standards regarding GMD and physical threats to the grid).

In some cases, system vulnerabilities and opportunities are strongly linked. For example, as energy systems become "smarter," incorporating more data and real-time feedback and control, vulnerabilities to cyber-attacks may increase. At the same time, increased information and communications technology may enable better system optimization, in turn reducing costs and improving environmental impacts. Ideally, systems should be robust and resilient to withstand or recover from extreme events like those discussed in the previous paragraphs.

---

[10] U.S. Department of Homeland Security (DHS). "Daily Open Source Infrastructure Report, 06 February 2014." February 6, 2014. DHS. Available at http://www.dhs.gov/sites/default/files/publications/nppd/ip/daily-report/dhs-daily-report-2014-02-06.pdf (accessed April 1, 2014)

[11] The Fukushima Nuclear Accident Independent Investigation Commission. 2012. *The Official Report of Executive Summary The Fukushima Nuclear Accident Independent Investigation Commission.* The National Diet of Japan. Available at http://www.nirs.org/fukushima/naiic_report.pdf (accessed April 1, 2014)

[12] U.S. Department of Homeland Security, Federal Emergency Management Agency (FEMA). 2013. *Hurricane Sandy: FEMA After-Action Report*. FEMA. Available at: http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf (accessed April 1, 2014)

[13] The Fukushima Nuclear Accident Independent Investigation Commission. 2012. *The Official Report of Executive Summary The Fukushima Nuclear Accident Independent Investigation Commission.* The National Diet of Japan. Available at http://www.nirs.org/fukushima/naiic_report.pdf (accessed April 1, 2014)

4. Shifting Assumptions Underlie Vulnerability Assessments

There are a number of drivers that are changing the boundaries of what should be considered normal operating conditions—thus affecting all three types of vulnerability. These include:

- **Aging Infrastructure:** One fundamental challenge to today's energy sector is that systems that were robust when they were newly built have aged and may have deteriorated, or they may be operating outside of the time or condition specifications for which they were initially designed. These effects vary by technology, use profile, etc. Some critical aging infrastructure components and systems are approaching or past their planned dates of retirement (e.g., extra high voltage transformers).[14] Underinvestment in maintenance means that systems which might have once been robust, could now be *systemically weak*.
- **Climate Change:** Climate change is another factor that is leading to more extreme weather and changing climatic conditions, thus forcing systems such as thermal power plants and the electrical grid to regularly operate under conditions that might have once been deemed unlikely or extreme.[15] In the longer term, increasing temperatures, decreasing water availability, more intense storm events, and sea level rise will each independently, and in some cases in combination, degrade the performance of energy systems.[16] For example, higher air and water temperatures reduce cooling efficiency and increasing power line losses. Changes in humidity can reduce the lifetime of infrastructure materials. Sea level rise may require relocation of energy facilities.
- **Infrastructure interdependencies**: Many critical energy (oil, natural gas, biofuels) and other infrastructures (telecommunications, water, transportation, and emergency services) are increasingly reliant on electricity. Other critical infrastructures—ports, harbors, waterways and rail—are also essential for the delivery of energy supplies to consumers. These interdependencies need to be more fully understood in order to develop comprehensive emergency and prevention protocols.

---

[14] U.S. Department of Homeland Security (DHS). "Power Hungry: Prototyping Replacement EHV Transformers." March 2, 2012. Available at: http://www.dhs.gov/power-hungry-prototyping-replacement-ehv-transformers (accessed April 1, 2014)

[15] U.S. Department of Energy (DOE), Office of Science. 2012. *Climate Change and Infrastructure, Urban Systems, and Vulnerabilities: Technical Report to the U.S. Department of Energy in Support of the National Climate Assessment*. DOE. Available at http://www.esd.ornl.gov/eess/Infrastructure.pdf (accessed April 1, 2014)

[16] National Oceanic and Atmospheric Administration (NOAA), Geophysical Fluid Dynamics Laboratory. "Global Warming and Hurricanes." December 30, 2013. Available at http://www.gfdl.noaa.gov/global-warming-and-hurricanes (accessed April 1, 2014)

5. Known Vulnerabilities

Some examples of known vulnerabilities for key energy sectors include:

	Systemically Weak	Vulnerable to attack	Vulnerable to extreme events
Liquid fuels	• Price volatility • Water dependency • Changes in Geographic distribution of resource and refining capacity	• Physical attacks (e.g. Libyan civil war) • SCADA used for safety or controlling loss of containment of toxic substances or flammable hydrocarbons	• Dependency on electrical system • Dependency on infrastructure like roads • Control facilities and ports located close to potential storm surges • Pipelines and forest fires, earthquakes
Gas	• Aging pipelines can result in catastrophic failures (e.g. San Bruno) • Systemic leakage • Constrained transmission	• Physical attacks on pipelines and gas processing facilities (e.g. Libyan civil war) • Pipelines are located in remote areas and difficult to continuously monitor • SCADA used for connecting distribution networks, safety, cost control, and billing	• Reliance on electricity infrastructure in some cases • Increased by climate-related events; water incursion, freeze-offs
Grid	• Regional fuel supply and fuel diversity issues • Regulatory barriers to transmission line construction, leading to congestion and difficulty in integrating • Utility business models • Large transformers are, on average, 40 years old • Cascading nature of grid impacts	• Cyber-attacks on electric infrastructure are increasing in frequency, and increased integration with IT systems may increase vulnerabilities • Physical threats may be shifting from vandalism (e.g. copper thefts) to terrorism	• Increased by climate-related events • Geomagnetic storms • Cost allocation issues • Who pays for grid hardening
Fuels Transport	• Aging and underfunded locks systems • Rail transportation risks • Monopoly abuses		• Barge and rail vulnerable to drought, flooding

6. Key Questions Regarding Energy System Vulnerabilities

Some key questions and issues the public may wish to address in comments to the QER Secretariat include:

- How do stakeholders view resilience challenges: what are the major vulnerabilities, what are available tools to address them, and where is policy intervention needed?
- To what extent is an aging/retiring workforce an issue? What sorts of programs can help address issues that exist?
- Are there ways to strengthen industry/government partnerships around cybersecurity issues, improving flows of information and data that are critical to protecting assets?
- What are the most critical system interdependencies, and how can stakeholders and policymakers address system weaknesses and vulnerabilities posed by these interdependencies?
- Are there specific policies, or policy gaps, that create vulnerabilities? Could these be addressed through specific executive or legislative action?
- Are there significant differences in the economic and other impacts of service disruptions to a specific user class (e.g. commercial, residential or industrial), duration or location?
- What new information do government and stakeholders need to support a resilient TS&D infrastructure?
- How much and what type of investment is needed in energy TS&D to ensure the safe delivery of electricity, natural gas, oil and liquid fuels, given the average age of the systems?
- What metrics are used to assess current conditions and measure improvements in resilience and security?
- How can government and industry accelerate appropriate resilience and security improvements?
- What financial, market or other incentives would encourage investment in resilience and security measures?
- What steps can be taken to make our energy infrastructure more resilient given demographic shifts to coastal areas prone to extreme weather?
- What are the key technology RD&D needs for risk mitigation, preparedness, recovery and response in the energy TS&D sector?
- How is climate change affecting particular components of our energy infrastructure? Which climate trends (e.g., sea level rise; increased risk of drought, flooding, storms, etc.) pose the greatest threat to our energy infrastructure? What are examples of costs and inefficiencies caused by climate change?