ADDENDUM

I. Overview[1]

The Nation's electricity grid has operated with a high level of reliability historically and continues to do so today. However, in light of the current threat environment and the evolving nature of the electricity system, reliability in the conventional sense is not sufficient. The grid also must be resilient and secure. The Nation's security and defensive capabilities, as well as critical infrastructure, depend on an electric grid that can withstand and recover from a major disruption, whether from an adversarial attack or a natural disaster. That ability to recover, known as the grid's resilience, in turn depends on the availability of robust and secure electric generation resources and their supportive supply chains.

In particular, resources that have a secure on-site fuel supply, including nuclear and coal-fired power plants, as well as oil-fired and dual-fuel units with adequate storage, are essential to support the Nation's defense facilities, critical energy infrastructure, and other critical infrastructure. Our national security also relies on a robust U.S. domestic industrial base, of which the coal, nuclear, and oil and natural gas industries are critical strategic components, as well as on a robust civilian nuclear power industry to support the entire U.S. nuclear enterprise and U.S. nuclear leadership abroad. A robust and secure network of natural gas pipeline infrastructure is also indispensable to the security of the Nation's electricity system.

Increasingly, however, due largely to regulatory and economic factors, too many of these fuel-secure plants have retired prematurely and many more have recently announced retirement. Although the lost megawatts of power often are replaced by new generation from natural gas and renewable energy sources, this transition comes at the expense of fuel security and resilience. As the North American Electric Reliability Corporation (NERC) states, "Premature retirements of fuel secure baseload generating stations reduces resilience to fuel supply disruptions."[2] Because the causes of this crisis primarily are regulatory and economic, prompt action by federal and state regulatory bodies and the private sector is required to achieve a lasting solution that meets the needs of both national security and the efficient operation of energy markets.

Under the [FAST Act], as part of its responsibilities as the Sector Specific Agency (SSA) for energy, the Department of Energy (DOE or the Department) is required to designate Critical Defense Facilities served by Defense Critical Electric Infrastructure (DCEI). To identify DCEI facilities, additional analysis will be required to gain a more detailed understanding of location-specific security vulnerabilities in our energy delivery systems, including the interdependencies associated with electric generation and transmission, and natural gas and petroleum pipelines, as well as their supply chains. DOE has begun the necessary analysis working with five National Labs. This analysis, which has never previously been undertaken, will take at least twenty-four months due to the complexity and inextricable dependency upon Canadian and Mexican system

---

[1] This Addendum is not an exhaustive statement of the analysis and reasons in support of the Department of Energy's action.

[2] North American Electric Reliability Corporation, *Synopsis of NERC Reliability Assessments: The Changing Resource Mix and the Impacts of Conventional Generation Retirements*, at 3 (May 2017) [hereinafter NERC Reliability Synopsis].

components of the interconnected North American grid. In the meantime, DOE's Order (the Order or Directive) provides a temporary stop-gap measure to prevent the further permanent loss of the fuel-secure electric generation capacity for the grid upon which our national security depends, much like the interstate highway system.

As the Sector-Specific Agency for Energy under Presidential Policy Directive-21 (PPD-21),[3] DOE has determined the following:

- Electricity generation capacity is increasingly dependent on natural gas pipelines, which represent a major point of vulnerability in our critical energy infrastructure due to the limits of protection available to thousands of miles of pipeline networks.

- Although the United States electricity system operates at a high level of "reliability" according to conventional reliability standards and metrics, it is widely recognized that the security and resilience of the system in the face of major disruptions goes well beyond reliability and requires a fundamentally different analysis.

- Growing threats of multi-point attacks, including cyber-attacks, or other disruptions to the energy sector, including the electricity grid and the natural gas pipeline system, are increasing the risk of high-impact events that could result in significant harm to human life, the economy, the environment, and national security.

- In addition to transmission capacity and other critical components of the bulk power system (BPS), fuel-secure electric generation capacity constitutes critical electric infrastructure within the meaning of the FAST Act.

- While intermittent resources (wind and solar) provide value at various times during the day, during times of peak demand when there is the greatest strain on the electricity grid, many major electricity markets are and will continue to be heavily dependent on fossil and nuclear electric generation resources.

- Recent and announced retirements of fuel-secure electric generation capacity across the continental United States are undermining the security of the electric power system because the system's resilience depends on those resources.

- Although additional analysis of location-specific impacts is needed, due to the interconnected nature of the electricity system it is necessary to maintain fuel-secure generating stations across each interconnection within the continental United States to ensure adequate system-wide resilience in the event of major disruptions.

- The entire U.S. nuclear enterprise—weapons, naval propulsion, non-proliferation, enrichment, fuel services, and negotiations with international partners—depends on a robust civilian nuclear industry. Without a strong domestic nuclear power industry, the

[3] *See* Presidential Policy Directive 21– Critical Infrastructure Security and Resilience, at 11 (Feb. 12, 2013), *available at* https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf.

U.S. will not only lose the energy security and grid resilience benefits, but will also lose its workforce technical expertise, supply chain, and position of clean energy leadership.

- Nuclear power, coal infrastructure, and pipeline infrastructure are all basic components of the Nation's domestic industrial base, which is necessary for national defense and furthers the National Security Strategy's priority goals of energy security through diverse supply and energy abundance.

To promote the national defense and maximize domestic energy supplies, federal action is necessary to stop the further premature retirements of fuel-secure generation capacity while DOE, in collaboration with other federal agencies, the States, and private industry, further evaluates national security needs and additional measures to safeguard the Nation's electric grid and natural gas pipeline infrastructure from current threats. To that end, as described below, it is necessary and appropriate for the Department to: (1) issue orders pursuant to its authority under the Defense Production Act of 1950 (DPA) and the Federal Power Act (FPA) to temporarily delay retirements of fuel-secure electric generation resources, while we (2) continue our analysis of, and take prompt action to address, the comprehensive resilience needs of our electric generation system, including specific actions to support defense critical energy infrastructure in the event of attack.

The Department is exercising its DPA and FPA authority by directing System Operators (as defined in the Directive), for a period of twenty-four (24) months, to purchase or arrange the purchase of electric energy or electric generation capacity from a designated list of Subject Generation Facilities (SGFs) sufficient to forestall any further actions toward retirement, decommissioning, or deactivation of such facilities during the pendency of DOE's Order. DOE also is directing SGFs outside of the RTO/ISO territories to continue generation and delivery of electric energy according to their existing or recent contractual arrangements with Load-Serving Entities. DOE's Order establishes a Strategic Electric Generation Reserve (SEGR) to promote the national defense and maximize domestic energy supplies. This prudent stop-gap measure will allow the Department further to address the Nation's grid security challenges while the Order remains in force.

II. Grid Resilience and National Security Threats

A. Resilience is Different from Reliability

It is widely agreed that the U.S. electric system operates at a high level of reliability.[4] It is also understood that most outages *to date* have been caused by distribution and transmission interruptions triggered by weather (including lightning strikes and hurricanes), lack of adequate vegetation management, and similar causes.[5] The Federal Energy Regulatory Commission (FERC), NERC, and other regulatory bodies, as well as utilities, have well-developed systems and metrics to evaluate and prepare for such events. Increasingly, however, it is also widely recognized

[4] *See e.g.*, National Academies of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation's Electricity System*, at 9 (2017) [hereinafter NASEM Study] ("The bulk power system achieves a relatively high degree of reliability across the United States as a whole.") .

[5] Department of Energy, *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*, at 4-28, 4-29 (Jan. 2017) [hereinafter QER]; see also NASEM at 56, 64.

that the security and resilience of the grid in the face of high-impact events caused by state actors, terrorists, or natural disasters go well beyond the conventional bounds of reliability.[6] Section 215 of the Federal Power Act provides for the establishment and enforcement of reliability standards by a FERC-approved Electric Reliability Organization (ERO). NERC currently serves as the ERO. Section 215 provides that the ERO establish standards for an "adequate level of reliability."

The statute does not specify "adequate" reliability, but does define "reliable operation" in terms that could be broad enough to encompass national security concerns.[7] Historically, however, NERC (with FERC's approval) has found it sufficient to set standards to ensure that the grid can operate in certain "credible contingencies"—*i.e.*, events that are expected and whose consequences are well understood. In NERC's narrow approach, credible contingencies involve the loss of a single system component. Under such contingencies, system operators are further required to plan for certain additional losses of system components, but not for the loss of a large number of components as would be likely in the event of a major attack or other disruption.[8] NERC's activity has developed to take into account a wider scope of likely events and includes certain planning requirements for "extreme" events.[9] NERC's own reliability assessments typically point to risks and threats that go well beyond its current standard.[10] Nevertheless, its current standards and metrics for reliability still do not adequately account for national security requirements. As Joseph McClelland, Director of FERC's Office of Infrastructure Security has testified,

> Section 215 of the Federal Power Act provides a statutory foundation for the ERO to develop reliability standards for the bulk power system. However, the nature of

---

[6] *See e.g., id.* at 4-33, 4-34.

[7] Section 215 defines "reliable operation" to mean "operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." [215(a)(4)]

[8] A recent FERC Staff Reliability Primer explains that, under current NERC standards, "[the] system must be operated at all times to ensure that it will remain in a secure condition (generally within emergency ratings for current and voltage and within established stability limits) following the unexpected loss of the most important generator or transmission facility (a 'single largest contingency'). This is called the 'N-1 criterion.' In other words, because a generator or line trip can occur at any time, the power system must be operated in a preventive mode. Use of the N-1 criterion means that the loss of the most important generator or transmission facility does not jeopardize the remaining facilities in the system by causing them to exceed their emergency ratings or stability limits, which could lead to a cascading outage." [RP at 22] Beyond N-1 events, "When a contingency does occur, system operators are required to identify and plan for the next contingencies based on the changed conditions.... Generally, the system must be restored to normal limits as soon as practical but within no more than 30 minutes, and to a condition where it can again withstand the next-worst single contingency.... Most areas of the grid are operated to withstand the concurrent loss of two or more facilities (i.e., 'N-2' or 'N-3'). This may be done, for example, as an added safety measure to protect a densely populated metropolitan area or when lines share a common structure and could be affected by the same event (e.g., a single lighting strike)." [RP at 22].

[99] [NERC has adopted standards for blackstart, cybersecurity, physical security and GMD, which have been criticized for being inadequate to the threats. But not EMP. Cite FRS, Woolsey, etc.]

[10] As discussed below, even while maintaining that the grid is currently "reliable," NERC identifies both cybersecurity and the loss of fuel-secure generation as "higher risk, higher likelihood" "risks."

> a national security threat by entities intent on attacking the U.S. by exploiting vulnerabilities in its electric grid using physical or cyber means stands in stark contrast to other major reliability events that have caused regional blackouts and reliability failures in the past, such as events caused by tree trimming practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. Given the national security dimension to this threat, there may be a need to act quickly to protect the grid in a manner where action is mandatory rather than voluntary while protecting certain sensitive information from public disclosure.[11]

In summary, as the National Academies of Sciences, Engineering, and Medicine Study concludes, "[a]lthough NERC standards have largely been effective in addressing credible contingencies and have been recently expanded to include consideration of extreme events, designing the grid to ride through catastrophic events such as major storms and cyber-attacks pushes their limit."[12]

The issue before the Department, then, is not whether our Nation's electric system has operated or is currently operating at a high level of *reliability*. Rather, it is whether the Nation's electric power system is adequately prepared and resourced to withstand a high-impact electricity system disruption caused by an attack, natural disaster, or other incident. This ability to withstand high-impact events is called "resilience." PPD-21 provides a general definition of resilience as it pertains to all critical infrastructures: "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." An adequate level of resilience for any critical infrastructure system must take into account the nature of the threats. , There is broad agreement among security experts, regulators, and energy industry experts that there is a need for greater resilience of the Nation's electric system to withstand an array of natural and intentional threats that are, in many cases, growing in frequency and scope. If the grid is not resilient to such disruptions, electric service may not be restored for a long time after a major disruption event. As NASEM states, "resilience is broader than reliability."[13] It should also be emphasized that, without resilience, there will likely be little or no reliability in the aftermath of the kinds of disruptions that are becoming ever more likely in the current threat environment.

The *resilience* of the electric power grid includes many components, and fuel security and diversity are among the most critical, as discussed below. In the fuel security context, the difference between conventional reliability metrics and a broader understanding of resilience. NERC, under FERC's oversight, regulates bulk power system electric reliability, but NERC does not have authority over natural gas pipelines and there are no mandatory reliability or security

---

[11] Testimony of Joseph McClelland, Director, Office of Energy Infrastructure Security, Federal Energy Regulatory Commission Before the Committee on Homeland Security and Governmental Affairs United States Senate, July 22, 2015, at 2. In the face of cyber, physical and other threats, "[t]he traditional definition of reliability—based on the frequency, duration, and extent of power outages—may be insufficient to insure system integrity and available electric power." QER at 4-4.

[12] *Id.* at 79 (citation omitted).

[13] NASEM Study, at 1.

standards for natural gas pipelines otherwise. The result is a situation in which conventional reliability standards do not adequately take into account gas pipeline vulnerabilities or related fuel security issues. In this context, market participants and other entities sometimes find themselves determining that the grid is "reliable" and, at the same time, that the grid is at serious risk from a fuel security standpoint. For example, on the same day that PJM approved a deactivation request for several nuclear generating units on the basis of its conventional reliability analysis, it issued a plan to initiate a study on "Valuing Fuel Security."[14] In this plan, PJM concluded that "**an increased reliance on any one resource type introduces potential fuel security risks not recognized under existing reliability standards**."[15] As defined by PJM,

> [F]uel security is the ability of the system's supply portfolio, given its fuel supply dependencies, to continue serving electricity demand through credible disturbance events, such as coordinated physical or cyberattacks or extreme weather that could lead to disruptions in fuel delivery systems, which would impact the availability of generation over extended periods of time."[16]

The goal of PJM's fuel security efforts is "to ensure that peak demands can be met during realistic but extreme contingency scenarios in various supply portfolios."[17]

Likewise, ISO New England has operated reliably in compliance with existing reliability standards and last fall stated that its capacity markets have accommodated retirements of coal-fired generation with "no adverse effect on regional resource adequacy or reliability of service."[18] However, only a few months later, commenting in FERC's resilience docket, ISO New England stated, "In New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability."[19] As a result, in New England, "Fuel constraints and the continued loss of major non-gas-fired generation may pose a threat to keeping the lights on during future cold snaps."[20]

FERC currently has an open proceeding on grid resilience, in which a vigorous discussion is taking place about the precise definition of "resilience" (as it applies to the bulk power system) and the relationship between resilience and reliability. Regardless of how these definitional debates are resolved, DOE, as a national security agency, takes a comprehensive, Intelligence

---

[14] PJM, *Valuing Fuel Security* (Apr. 30, 2018).
[15] *Id.* at 1.
[16] *Id.*
[17] *Id.* at 2.
[18] [ISO NE Comments in FERC Docket RM18-1]
[19] [ISO NE Response to Grid Resilience in RTO and ISOs (AD18-7-000), March 9, 2018, p. 1][See also ISO NE Operational Fuel Security Analysis p 4: "**Fuel-security risk**—the possibility that power plants won't have or be able to get the fuel they need to run, particularly in winter—is the **foremost challenge to a reliable power grid in New England.**]
[20] *Id.* at 11. "The retirements of coal-fired, oil-fired, and nuclear generators—resources with fuel stored on site—will have a significant impact on reliability and magnify the importance of other variables, particularly liquefied natural gas (LNG) supplies." [p4]

Community informed view of resilience within the context of national security. To be prepared to withstand major disruptions, the electricity system must not only operate reliably in the conventional sense, but it must also be resourced to withstand and recover from major disruptions caused by multi-point attacks or other increasingly likely events of unprecedented magnitude and scope.

B. Current Adversarial Threats to Critical Infrastructure

The President's National Defense Strategy states, "It is now undeniable that the *homeland is no longer a sanctuary*. America is a target . . . . During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."[21] The threats to our critical energy infrastructure include intentional attacks by state actors and other enemies, as well as extreme weather and natural disasters. More specifically, the President's National Security Strategy states, "[t]he vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication."[22]

1. Threats to the Energy Subsector

PPD-21 identifies the Energy Sector as "uniquely critical due to the enabling functions [it] provide[s] across all critical infrastructure sectors."[23] The Nation's energy infrastructure faces a growing range of hazards, from increasingly sophisticated physical and cyber threats, to severe weather events and natural disasters, among others.[24] The evolving risk associated with mitigating cyber and physical security challenges is one of the most pressing issues for the sector. The sector has seen the occurrence of a number of each type of incident in recent years. According to NERC, "cyber and physical security threats are increasing and becoming more serious over time."[25]

A number of factors exacerbate the energy sector's cybersecurity challenge. The growing use of automated controls to operate energy systems, along with expanding knowledge and capabilities of malicious cyber actors, have increased the risks faced by both electricity and oil and natural gas facilities . The vulnerabilities of industrial control systems to cyber-attacks is one of the chief concerns for the Nation's critical infrastructure owners and operators. The use of information technology and operational technology components that share many of the same characteristics in terms of both their hardware and software also increase risks to the sector. Not only are individual components of concern, but also the interconnections between them—which can vary widely as new and old components are used together in systems.

---

[21] Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, at 3 (emphasis in original), *available at* https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[22] National Security Strategy of the United States of America, at 12 (Dec. 2017), *available at* https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[23] PPD-21 at 2.

[24] *See* Figure 2, below. The source is NERC, *ERO Reliability Risk Priorities: RISC Recommendations to the NERC Board of Trustees*, fig. 2.1, at 11 (Feb. 2018), *available at* https://www.nerc.com/comm/RISC/Documents/ERO-Reliability-Risk-Priorities-Report.pdf.

[25] North American Electric Reliability Corporation, *2017 Annual Report*, Feb. 2018, at 9, *available at* https://www.nerc.com/gov/Annual%20Reports/2017%20Annual%20Report.pdf.

Based on incidents reported by energy sector participants in the Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the U.S. energy sector is one of the Nation's most highly targeted critical infrastructure sectors for cyber adversaries.[26] Energy sector stakeholders in both government and industry perform regular assessments, exercises, and information sharing and coordination in response to the growing cyber threat. Cyberattacks and intrusions targeting U.S. electric utilities have been reported, and the enhanced cyberattack capabilities in Russia, China, Iran, and North Korea represent a growing threat.[27] Criminal operations based abroad have recently targeted critical organizations—for instance, the Iran-based cyberattack on the Federal Energy Regulatory Commission—and such threats are likely to increase.[28] The physical security risk to the energy sector includes the potential for adversaries to inflict "intentional damage, destruction, or disruption to facilities."[29] The dispersed and exposed nature of many components of the electric grid, such as substations or transmission lines, as well as pipelines, makes infrastructure difficult to protect. Although these intrusions have not yet resulted in verified physical damage or disruption to energy infrastructure control systems in the United States, the capability of our adversaries to cause such disruptions appears to be increasing.[30]

---

[26] *See* Supplement, at note ii.

[27] *See* Worldwide Threat Assessment 2018, *available at* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf; https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[28] *See* Press Release, U.S. Dep't of Justice, Office of Public Affairs (Mar. 23, 2018) (describing indictment of nine Iranian nationals using an Iranian company to steal more than 31 terabytes of data from hundreds of universities, dozens of private sector companies, and government agencies, including FERC, mostly "on behalf of [Iran's] Islamic Revolutionary Guard Corps"), *available at* https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary (last visited May 14, 2018).

[29] *See* North American Electric Reliability Corporation, *ERO Reliability Risk Priorities: RISC Recommendations to the NERC Board of Trustees*, 10 (Nov. 2016).

[30] *See* Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report* (Idaho Falls, Idaho: Idaho National Laboratory), Aug. 2016, at 4. Recent examples of widely reported cyber incidents include: (1) VPNFilter (Reported on May 23, 2018, by Cisco Talos Intelligence Group that an unidentified hacking group has infected over 500,000 routers in 54 countries with malware that has code that overlaps with versions of the BlackEnergy malware that previously was used to sabotage the Ukrainian power grid. *See New VPNFilter malware targets at least 500K networking devices worldwide, available at* https://blog.talosintelligence.com/2018/05/VPNFilter.html, *see also* #7); (2) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure (Per DHS' and the FBI's March 15, 2018 Joint Technical Alert, "Russian government cyber actors" targeted government entities and multiple U.S. critical infrastructure sectors, including the energy and nuclear sectors, by staging malware, conducting spear phishing, and gaining remote access into energy sector networks, collecting information pertaining to ICS) (*See* United States Computer Emergency Readiness Team, Alert TA18-074A, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (Mar. 15, 2018), available at https://www.us-cert.gov/ncas/alerts/TA18-074A); (3) attack on Eirgrid, Ireland's electricity wholesale transmission system operator Reported on August 6, 2017, that hackers installed eavesdropping software (Generic Routing Encapsulation (GRE) tunnel) on routers of Eirgrid, the state-owned company that

2. Threats to the Natural Gas Subsector

As has been widely reported, natural gas pipelines are increasingly vulnerable to cyber- and physical attacks.[31] Using a standard risk-based analysis, NERC has identified the disruption of electric generation supplied by gas pipelines as both a higher impact and higher likelihood event, due to the supply chain components required to provide adequate gas supply to electric power

---

manages and operates the wholesale transmission electricity grid in Ireland and hackers were able to capture Eirgrid's encrypted communications. *See* Cathal McMahon, *Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'*, The Independent, *available at* https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html); (4) spear phishing attack of Irish electric utility (On July 17, 2017, it was reported that senior engineers at the Electricity Supply Board, a state-owned utility which supplies electricity to Northern Ireland and the Republic of Ireland, were sent personalized emails containing malicious software "by a group linked to Russia's GRU intelligence agency." *See Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure*, *available at* https://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html); (5) CrashOverride/Industroyer (On June 13, 2017, NERC issued a Level 1 NERC Alert to inform the electricity sector of capabilities found in malware targeting electric industry assets in Ukraine. The malware was designed to cause loss of visibility, loss of control, manipulation of control, interruption of communications, and deletion of local and networked critical configuration files. CrashOverride was associated with the cyber-attack which caused outages in the Ukrainian city of Kiev in December 2016.) (*See* North American Electric Reliability Corporation, *Industry Advisory: Modular Malware Targeting Electricity Industry Assets in Ukraine* (June 13, 2017), *available at* https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERCAlert_A-2017-06-13-01_Modular-Electric-Industry-Malware.pdf); (6) Grizzly Steppe (December 29, 2016 Joint Analysis Report by DHS and the FBI details tools used by Russian intelligence services to compromise and exploit networks and endpoints in the U.S.) (*See* Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity (Dec. 29, 2016), available at https://www.fbi.gov/news/pressrel/press-releases/joint-dhs-odni-fbi-statement-on-russian-malicious-cyber-activity); and (7) BlackEnergy (On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. Power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers. BlackEnergy is a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks, among other tools to compromise information.) (*See* United States Computer Emergency Readiness Team, IR-ALERT-H-16-056-01, Cyber-Attack Against Ukrainian Critical Infrastructure (Feb. 25, 2016), available at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01).

[31] See, e.g., "Cyberattack Shows Vulnerability of Gas Pipeline Network," New York Times, April 4 2018 https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html. Blake Sobczak, Hannah Northey and Peter Behr, "Cyber raises threat against America's energy backbone," *E&E News*, May 23, 2017, https://www.eenews.net/stories/1060054924/; Blake Sobczak, "FERC Commissioner Sounds 'Call for Action' on Pipelines," E&E News, May 29, 2018. https://www.eenews.net/energywire/2018/05/29/stories/1060082831

generation units.[32] Specifically, the incapacitation of certain pipelines throughout the United States would have severe effects on electric generation necessary to supply critical infrastructure facilities.

Further, many natural gas and petroleum pipelines are designed to operate to provide one-way commodity flow. Thus, there is an increased susceptibility because a disruption at the "head end" of the pipeline disrupts the flow to all downstream pipeline facilities. Although there is redundancy built into the system, the present design of the system nonetheless poses significant risks associated with supplying commodity services to ensure national and economic security. Two-thirds of the lower 48 States are almost entirely dependent on the interstate pipeline system for their supplies of natural gas.

Natural gas, petroleum, and coal are all, to varying degrees, dependent upon supply chain interfaces that are each exposed to cyber and physical threat. However, this exposure is minimized where electric generation facilities are able to maintain fuel stockpiles onsite, as with coal and nuclear. From a resilience and national security risk perspective, those facilities that are able to secure key fuel commodities represent an important safeguard in this context, as discussed in more detail below.

Additional information regarding serious and sophisticated threats to the energy sector is contained in classified documents available to certain personnel of the Department and maintained by the Office of the Director of National Intelligence.

III. The Grid's Vulnerability Due to Loss of Fuel-Secure Generation Capacity

In light of these increasing and sophisticated threats to the energy sector, DOE continues to evaluate the resilience of the electric grid and the impacts of the ongoing loss of fuel-secure generation capacity.

The electric power system in the lower 48 States is comprised of three main "interconnections" spanning the lower 48 States– these are the Eastern and Western Interconnections, and the Electric Reliability Council of Texas.[33] Each of these interconnections is a single integrated machine that must operate continuously and at a high level of capacity to maintain stability. The three interconnections are electrically independent from each other (except for a few small DC ties). Although these are referred to as "the grid" or "grids," each is composed not only of high-voltage transmission wires, but also of electric generation units (power plants), substations, control centers, communications equipment, etc. The system as whole includes both

---

[32] *See* NERC, *ERO Reliability Risk Priorities: RISC Recommendations to the NERC Board of Trustees*, at 18 (noting that "[t]he resource mix and its delivery is transforming from large, remotely-located coal and nuclear-fired power plants, towards gas-fired . . . and other emerging technologies" and warning that "[t]hese changes in the generation resource mix and the integration of new technologies are altering the operational characteristics of the grid and will challenge system planners and operators to maintain reliability.")

[33] FERC Staff Reliability Primer at [**]. These comprise also portions of Canada and Mexico. The Quebec Interconnection is a fourth distinct interconnection. Neither Alaska, Hawaii, nor the island territories of the U.S. are connected to the lower 48 BPS.