U.S. Senate Committee on Energy and Natural Resources
June 26, 2018 Hearing: *Pending Nominations*
Questions for the Record Submitted to Ms. Karen S. Evans

Questions from Chairman Lisa Murkowski

Question 1: This month Secretary Perry and Israeli Energy Minister Steinitz signed an agreement to establish the U.S. – Israel Research and Development Center, a joint energy research program between our two nations. One of the primary focuses of the Center is on energy cybersecurity. What role will CESER have in promoting that joint research? More broadly, what level of coordination do you see CESER having with our international partners, particularly with our North American neighbors?

Answer: If confirmed, I look forwarding to learning more and partnering with our international allies. I am unclear on the role CESER will play in international cybersecurity agreements, but I believe it is critical we share information with our allies regarding threats and system improvements mitigating threats and reducing risks to the energy infrastructure.

Question 2: I understand that there are many people in industry awaiting security clearances – what role do you think that you will be able to play in encouraging a better process at ensuring the right people have a clearance at the right time?

Answer: I have not been fully briefed on this issue and I look forward to learning more should I be confirmed as Assistant Secretary. Industry stakeholders having the appropriate clearance is a critical factor for information sharing as it relates to cyber threat mitigation.

Question 3: The Committee heard testimony at its March 1, 2018 hearing on cybersecurity risks for the energy sector that there is a need for what has been called consequence-driven cyber-informed engineering or CCE. The idea behind CCE is to lead to systems and equipment for industrial control that are designed and built with an understanding of cyber threats and risks such that those systems can be more readily defended. What is your view of CCE and are you open to making it a priority? If so, would multi-year funding enable greater operational support for CCE?

Answer: It is my understanding the idea behind CCE is to engineer out the cyber risk from the systems based on determining critical functions and high consequence events by understanding the vulnerabilities with the control systems. If confirmed, I would look forwarding to learning more about CCE in order to determine the appropriate processes and priorities for the reduction of cyber threats and risks associated with the energy infrastructure. I would work with Congress in accordance with the Department's budget processes to recommend the appropriate funding level request.

Question 4: I can envision two types of training for a cybersecurity attack. The first would involve the Information Technology (IT) specialists that work behind the scenes in keeping computers up and running throughout the grid. The second would involve the actual operators of those computers.

- What are your objectives in ensuring that both will have access to the best training that they can get?

  Answer: The main objective is to ensure sustainability of our energy infrastructure during a cybersecurity incident. In order to accomplish this result, if confirmed, I would leverage existing training programs, address gaps in the training programs which could be identified through exercising existing response plans and adjust the training programs. As the threats are constantly changing, the training would need to be adapted to address reducing the associated risks.

- Do you think that cybersecurity training for our grid operators is sufficient at this time? What needs to be improved?

  Answer: I am not fully briefed on this issue at this time but should I be confirmed, I look forward to learning what type of training is in place as our grid operators should have the necessary skill sets in order to have situational awareness of the risks associated with their environment.

- Does training need to reach down to all grid operators, and not just a few?

  Answer: Just like system redundancy can mitigate cyberattacks, training redundancy can as well by ensuring all employees and stakeholders have the relevant skills sets to identify and mitigate an intrusion.

Questions from Ranking Member Maria Cantwell

Question 1: Over the past year, my colleagues and I have sent two letters to the President asking for an increased focus at DOE on cyber threats to energy infrastructure. While I appreciate the focus of the new CESER office, I am not convinced that the actions of the administration have kept pace with its rhetoric. True, the Cybersecurity for Energy Delivery Systems budget line item received a marginal 13 percent increase in funding in DOE's budget request. But that is not nearly enough to keep pace with the ever evolving threats. And the money is being taken out of other critical offices for grid reliability.

—The Transmission Reliability and Resilience Office is being reduced by 64 percent;

—the Resilient Distribution Systems office is being slashed by 80 percent.

Compare these numbers to this Committee's bipartisan energy bill that would double funding for cybersecurity at DOE without decreasing funding for other resilience programs.

- If confirmed, how will you make sure that DOE's focus on cybersecurity keeps pace with the evolving threat?

Answer: By creating CESER, Secretary Perry is elevating the issue and I look forward to the challenges of running a new office with such an important mission, if confirmed. Information sharing with Congress and industry will be a major focus in addressing the evolving threat.

- How will you do so given the modest funding increase, which comes at the expense of other resilience programs?

  Answer: Many of the threats associated with the energy infrastructure can be addressed by ensuring basic hygiene is maintained for systems. Having situational awareness through information sharing with the private sector would assist in the resiliency needed.

Question 2: The new Cybersecurity, Energy Security, and Emergency Response office will have vast and critical responsibilities in addition to cybersecurity. The Infrastructure Security and Energy Restoration responsibilities include coordinating a national effort to secure U.S. energy infrastructure against all hazards, and coordinate emergency response efforts. In an energy crisis such as the one this country is still experiencing in Puerto Rico, your office will be in the national spotlight and the lives of potentially millions of Americans will be at stake. In Puerto Rico, the inability of patients to refrigerate their insulin and power their nebulizer machines have had devastating and fatal consequences. Given your IT background, but apparent lack of experience in energy infrastructure emergency response and coordination, how will you ensure that the federal government is fulfilling its duties in potential life threatening crises?

Answer: I have not been fully briefed on the Department's specific role in the Puerto Rico recovery process. From what I understand, one of the divisions of CESER, Infrastructure Security and Emergency Response (ISER), plays a critical role in the immediate response to emergencies that have affected energy infrastructure. However, I believe my IT experience is applicable as the concepts and skills are the same as many of the systems I have supported in the past were mission critical and needed to be operational at all times. If confirmed, I look forward to learning more about the Department's role in the disaster relief process, specifically the role ISER has in the process.

Question 3: I am particularly concerned about the threat Russia poses to the electric grid. Last year in Congressional testimony Admiral Michael Rogers suggested that Russia holds the cyber capability to cripple our infrastructure. In December 2015 and 2016, the Russians allegedly hacked several Ukrainian utilities, blacking-out hundreds-of-thousands of customers for several hours. Last June, I led a letter with 18 of my Senate colleagues requesting a thorough threat and vulnerability assessment with respect to Russia and U.S energy infrastructure. I and several of my colleagues received a classified briefing, but our group of 19 Senators is still awaiting a formal, public, written response to our request dated June 22, 2017 to President Trump and Secretary Perry. If confirmed, will you ensure that the 19 Senators, 6 of whom sit on this committee, receive a formal, written, public response that we and the country deserve?

Answer: If confirmed, I look forward to being briefed on this issue in order to provide an appropriate response to the Congressional request.

Question 4: The CEDS cyber R&D program has a substantial track record in delivering key innovations with industry and utilities to harden the power system. This success is due in large part to strong engagement with other aspects of the OE R&D portfolio related to grid operations, control and protection systems developments. How do you envision maintaining this strong connection between cyber R&D and the balance of grid R&D within OE?

Answer: If confirmed, I believe one of my top priorities will be ensuring a close working relationship with OE. Establishing a positive working relationship in the early months of the formation of the Office will address the concern of maintaining the connection into the future.

Question 5: Security and resilience are a fundamental part of the DOE Grid Modernization Initiative which spans OE, FE, EERE, NE and now CESER. It has over 100 industry and state partners and strong support by this Committee. Please share your vision for how the CESER charter aligns with the Grid Modernization Initiative and its multi-year program plan, and your level of commitment to ensuring that CESER contributions to the overall Grid Modernization Initiative.

Answer: I am not fully briefed on the Department's Grid Modernization Initiative. If confirmed, I look forward to learning and participating collaboratively with the program offices within the department as well as the national laboratories, universities and private sector as appropriate.

Question 6: In the above referenced June 22 letter to President Trump and Secretary Perry, 19 Senators requested within 60 days an analysis of: a) the scope of Russian capabilities to use cyber-warfare to threaten our energy infrastructure; and b) the extent to which the Russians have already attempted cyber-intrusions into our electric grid, pipelines, and other important energy facilities. In previous hearings I have called for a cyber vulnerability and cyber threat assessment to be performed with respect to the nation's energy infrastructure.

The executive order that I believe you referenced at today's hearing ("Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" of May 11, 2017) does not in any way address what I have called for. Instead, the executive order called for an assessment of "Electricity Disruption Incident Response Capabilities" which focuses solely on an assessment of the consequences of an incident, and not the threats posed to energy infrastructure or the specific vulnerabilities of the infrastructure to such threats.

Recognizing that the referenced executive order and the administration's response to the order does not address what I have called for, do you believe a vulnerability and threat assessment needs to be performed? When will you be able to present such an assessment to the committee?

Answer: At the hearing I also referenced the "Worldwide Threat Assessment" which includes a cyber component. From what I understand based on question #3, you received a classified briefing that highlighted the threats to our energy infrastructure. If confirmed, I look forward to working with your staff on this issue and the information you seek.

Questions from Senator Ron Wyden

Question 1: I believe that multi-factor authentication is critical for cybersecurity. Right now, agencies are only required by the Federal Cybersecurity Enhancement Act of 2015 to utilize multi-factor authentication for administrative accounts on agency information systems. I think that multi-factor authentication should be required for all agency employees accounts.

If confirmed, would you advocate for DOE to utilize multi-factor authentication for all employee accounts on agency information systems?

Would you also evangelize the importance of multi-factor authentication to the energy sector?

Answer: Multi-factor authentication for information systems reduces risks. If confirmed, I look forward to working with you and your staff to ensure the Department's information systems are as safe as possible and addressing the importance of level of security for the energy sector as well.

Question 2: According to public reports, there is a lengthy backlog for DOE clearances. This means that many of the tech experts working for energy companies can't see the classified cyber threat data that DOE shares with the energy industry.

How concerned are you about this clearance backlog and its impact on energy sector cybersecurity?

Answer: I have not been fully briefed on this issue and I look forward to learning more and addressing this issue in an appropriate manner should I be confirmed as Assistant Secretary.

If confirmed, what will you do to speed things up?

Answer: I have not been fully briefed on this issue and I look forward to learning more should I be confirmed as Assistant Secretary. I also look forward to working with you and your staff to reach a viable solution.

Question 3: DOE is considering an emergency order to support coal and nuclear power plants, arguing they are necessary for the energy security of the United States. This contradicts the position of grid operators such as the PJM Interconnection, which said there is no immediate threat to system reliability. The effect this order would have is raising Americans' utility bills, potentially by as much as $65 billion per year.

If confirmed, what range of stakeholder input would you consider if you were asked to determine whether the retirement of coal and nuclear plants threatens the energy security of the United States?

Answer: I have not been fully briefed on this issue and I look forward to learning more and addressing this issue in an appropriate manner should I be confirmed as Assistant Secretary.

Question 4: Part of the mission of this new office is responding to energy emergencies. Hurricanes Irma and Maria had a terrible impact on the grids on Puerto Rico and the U.S. Virgin Islands, and caused suffering for millions of Americans.

Given that your background is in information technology and cybersecurity, what specific steps will you take so that you are prepared to respond to energy emergencies?

What lessons from the response to Hurricanes Irma and Maria will you use to improve DOE's response to future emergencies?

Answer: I have not been fully briefed on the Department's specific role in the Puerto Rico recovery process. From what I understand, one of the divisions of CESER, Infrastructure Security and Emergency Response (ISER), plays a critical role in the immediate response to emergencies that have affected energy infrastructure. However, I believe my IT experience is applicable as the concepts and skills are the same as many of the systems I have supported in the past were mission critical and needed to be operational at all times. If confirmed, I look forward to learning more about the Department's role in the disaster relief process, specifically the role ISER has in the process.

Questions from Senator Joe Manchin III

Questions: As you may know, in 2015 and 2016, Ukraine experienced attacks on its power grid. These attacks moved across energy infrastructure and, because of the interdependencies the electric grid with other systems, an entire region was quickly and easily affected. Because of recent attacks in the US, my concern is only growing as these attacks are reportedly becoming more frequent and more complex.

From your perspective, what has been the single most helpful strategy or approach in helping owners and operators to stop these attacks in time to mitigate damage?

As you see it, are there policies at the federal or state level that you believe are hindering the ability to address cyber security?

Answer: The cyber threat landscape is constantly changing. It is important for owners and

operators to understand their operating environment and the associated risks. With this understanding, they would be able to implement risk mitigation plans to identify the attacks and implement appropriate responses. If confirmed, I look forward to reviewing DOE's role in helping prevent such attacks or the quick recovery from such attacks.

Questions from Senator Martin Heinrich

Question 1: Under sec. 215 of the Federal Power Act, the electric utility sector is the only critical infrastructure sector that has mandatory and enforceable standards for cybersecurity. However, the security of the interstate gas pipeline system shares many of the same control and data acquisition systems as power generators and the transmission grid. In your opinion, given the increasing dependence on natural gas in power generation, are current cybersecurity protections for natural gas pipelines sufficient? Or are additional or even mandatory measures needed to protect the interstate gas pipelines used for power generation?

Answer: Similar to the electric sector, physical and cybersecurity of crude oil, petroleum, and natural gas pipelines are critical. The Fixing America's Surface Transportation Act (FAST Act) codifies the role of the Department as the Sector-Specific Agency for energy cybersecurity. If confirmed, I look forward to working on ensuring pipeline security by working with industry and government partners.

Question 2: Investment in new power transmission infrastructure is essential to the future deployment of new pollution-free generation that will boost energy security and help diversify our power generation resources. What do you see as DOE's role in encouraging regional planning and investment in new transmission infrastructure that will enhance the reliability and resilience of the grid?

Answer: Investments in grid security and resilience, where needed, are critical to the security of our Nation and the affordability of electricity. If confirmed, I look forward to learning more about the Department's role in this space.

Questions from Senator Mazie K. Hirono

Question 1: Your testimony highlighted your past efforts on building up a cybersecurity workforce. The University of Hawaii and other colleges in my state have set up degree programs to meet the demand for qualified people to work in the Department of Defense, the private sector, and elsewhere. What lessons would you bring about cybersecurity workforce development, and how would you change what DOE is doing on the issue?

Answer: Ensuring a skilled cybersecurity workforce of the future is critical for the security of our energy infrastructure and the Nation as a whole. If confirmed, I look forward to ensuring DOE takes every opportunity to work towards achieving that goal.

Question 2: As industrial control systems used in the power grid, pipelines, and other infrastructure become more complex, they becoming more connected and potentially more vulnerable. On the other hand, technical advances could potentially make these systems easier to protect because they can incorporate the latest state of the art security technology such as advanced encryption algorithms and other measures. In your opinion, is progress being made to ensure industrial control systems in the energy industry are more secure as the technology becomes better, or are we losing ground because these systems are becoming more complex and inherently more vulnerable to advanced persistent cyber threats?

Answer: The interdependencies of industrial control systems makes the energy sector more vulnerable to attack. Increasing the redundancy of these systems can make our critical infrastructure more secure, but not immune to cyberattacks. As these systems continue advance, it is possible to use machine-to-machine event management to identify and mitigate risks.

Question 3: In your view, how can the federal government help utilities and other energy industry members better understand and respond to cybersecurity threats?

Answer: Many of the threats associated with the energy infrastructure can be addressed by ensuring basic hygiene is maintained for systems. Having situational awareness through information sharing with the private sector would assist in understanding of cybersecurity threats in order to respond to the increasing risks.

Question 4: As an island state, Hawaii shares many of the same vulnerabilities of Puerto Rico, starting with the fact that each island is its own grid. If confirmed, you would be responsible for leading DOE's efforts to help restore power and other emergency response efforts. What have you learned from the federal government's response to the large-scale loss of power in Puerto Rico after last year's hurricanes, and how will you help speed up the pace of getting energy resiliency solutions in place if you are confirmed?

Answer: It is my understanding the Department recently released their report regarding the response and support of Puerto Rico. If confirmed, I look forward to learning about the lessoned learned in the Department's response and applying them for future emergency response efforts.

Question 5: To ensure the fitness of nominees for any of our appointed positions, I ask every nominee who comes before me to answer the following two questions:

a. Since you became a legal adult, have you ever made unwanted requests for sexual favors, or committed any verbal or physical harassment or assault of a sexual nature?

   Answer: No.

b. Have you ever faced discipline, or entered into a settlement related to this kind of conduct?

Answer: No.

Question from Senator Tammy Duckworth

Question: The newly created Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is tasked with protecting our energy infrastructure from natural disasters and other security threats. 2017 has already experienced a significant number of natural disasters, including heat waves, hurricanes, flooding and drought. Extreme weather events heavily tax the grid and threaten consumers' access to reliable electricity. As the United States Geological Survey observed:

"With increasing global surface temperatures the possibility of more droughts and increased intensity of storms will likely occur. More heat in the atmosphere and warmer ocean surface temperatures can lead to increased wind speeds in tropical storms. Rising sea levels expose higher locations not usually subjected to the power of the sea and to the erosive forces of waves and currents."

Ms. Evans, if confirmed to be Assistant Secretary of CESER, how will you direct the Office to address the growing threats to the electric grid from climate change?

Answer: From what I understand, CESER focuses on coordinating preparedness and response to cyber and physical threats and natural and man-made disasters to the energy infrastructure. If confirmed, I look forward to looking into this and working with your staff.

Questions from Senator Catherine Cortez Masto

Question 1: On January 8, the Federal Energy Regulatory Commission (FERC) unanimously rejected DOE's grid resiliency proposal to provide support for failing coal and nuclear plants, saying there is no evidence that any past or planned retirements of coal-fired power plants pose a threat to reliability of the nation's electric grid. Subsequently, a leaked DOE memo from May 28 would compel grid operators to buy electricity from at-risk plants under the auspices of national security. Considering there is no emergency to respond to, it's hard to envision how propping up at-risk coal and nuclear plants might be implemented under the auspices of national security. What would such an emergency look like that would keep these plants online, that couldn't be rectified with the grid system and resources we already have today?

A. Do we know for sure that keeping obsolete plants would provide a benefit to the electric grid?

   Answer: I was not involved in the decision making processes for either the proposal or the leaked memo cited above. However, baseload generation, such as coal, nuclear, and hydropower, provide cheap, reliable energy to the grid. This office is to address energy security by ensuring the nation has ample resource adequacy that can help prevent and

recover from emergencies, such as cyberattacks to the grid. If confirmed, I look forward to learning more about this issue and providing the necessary information to the appropriate policy makers.

B. Since there is no energy shortage and these plants are not low-cost generators, is it possible that these plants would be kept from retirement – yet also not generate any power?

Answer: I am not fully briefed on this issue and if confirmed, I look forward to learning more and providing the necessary information to the appropriate policy makers.

C. If the plants are neither retired nor generating power, what would the net effect be on employment and rates in the related markets? Essentially, who would be benefitting, just the owners?

Answer: I am not fully briefed on this issue and if confirmed, I look forward to learning more and providing the necessary information to the appropriate policy makers.

Question 2: Are there vulnerabilities to cleaner energy sources, such as natural gas or renewables, as that other power sources do not experience, or vice-versa? For instance, is cyber security somehow a larger concern for these resources than for coal or nuclear?

Answer: Natural gas pipelines add another level of vulnerability as they are susceptible to attack. Renewable sources are variable and integrating them onto the grid is more difficult because sometimes supply and demand do not match. As all delivery systems rely on technology and become more complex, risks and vulnerabilities will continue to increase. If confirmed, I look forward to learning more about energy sources and potential associated risks in order to provide the necessary information to the appropriate policy makers.

Question 3: Would you agree that there is no industry immune to cyber threats?

Answer: Yes

Question 4: Shouldn't we should be focusing our resources on the resilience of the system rather than propping up companies that aren't economically viable under the veil of national security?

Answer: The resilience of the electric system is paramount and if confirmed, I will commit to work to ensure we have a reliable, resilient grid.

Question 5: It is my understanding that 96 percent of electricity outages are from transmission and distribution problems, not from a lapse in generation. Under your leadership, what would CESER do to create a stronger, more resilient electric grid?

Answer: From what I understand, traditional outages on the transmission and distribution system is more within the jurisdiction of the Office of Electricity, Delivery, and Energy Reliability at the Department.

Question 6: How will you work with DHS and DOE's Hydropower Program in the Water Power Technologies Office (housed within the Office of Energy Efficiency and Renewable Energy – EERE) to address threats to our hydropower facilities?

A. Can you elaborate on the respective authorities and responsibilities in this context?

   Answer: It is my understanding that DOE works with DHS in their role as the Sector Specific Agency for the energy sector to address these threats. If confirmed, I look forward to learning more about the specific threats to ensure associated roles and responsibilities are appropriately addressed.

B. In your view, how are the threats to our water and power infrastructure assets evolving over time?

   Answer: I am not fully briefed on the threats at this time in this area. If confirmed, I look forward to gaining a better understanding of the threat landscape.

C. What resources are further required to meet the threat today and in the future?

   Answer: I am not fully briefed on the threats at this time. If confirmed, I look forward to conducting the analysis to identify the necessary resources to address the threat on an on-going basis.

D. What are some of the threats you see that aren't getting enough attention?

   Answer: I am not fully briefed on the threats at this time. If confirmed, I look forward to conducting this analysis and working your staff to address concerns you may have.

Question 7: In 2017, the State of Nevada created the Office of Cyber Defense which serves as the primary focal point for cyber threats and security across the state. Along with the State Cyber Defense Coordinator, this office serves as the primary conduit with the federal government, as well as the primary entity managing cyber threat issues across the State of Nevada. How can the federal government best coordinate with State cyber offices like Nevada's to perform cyber threat analysis and reporting of threat information?

Answer: Based on my experience, the Multi-State ISAC shares information from multiple sources such as DHS with state, local and tribal governments. Additionally, it is my understanding DOE has information sharing resources as well and this information coordinated with DHS. If confirmed, I look forward to learning more regarding our efforts for sharing information in order to better coordinate preparedness and response to incidents.

Question 8: I am very concerned that the White House recently eliminated the cybersecurity advisor role and separated those responsibilities to two lower-level staffers. Eliminating this role only increases the concern that this administration is short-handed and unprepared to deal with increasing cybersecurity threats. Does the threat from cyber security attacks, whether it be on the electric grid, transportation systems, electoral systems, corporate assets, etc. not warrant a heightened level of prominence within the highest levels of decision-making for our country?

A. Would you recommend reinstating this position?

Answer: The cybersecurity threat is real and that is why Secretary Perry has created this Office for which I have been nominated to lead. If confirmed, I would ensure the Secretary and other policy makers receive the appropriate information regarding threats to the energy infrastructure for decision-making.