**TESTIMONY OF TRISTAN VANCE, DIRECTOR,**

**INDIANA OFFICE OF ENERGY DEVELOPMENT;**

**CHIEF ENERGY OFFICER OF INDIANA, BEFORE**

**THE U.S. HOUSE ENERGY SUBCOMMITTEE OF THE**

**COMMITTEE ON ENERGY AND COMMERCE IN SUPPORT OF**

**LEGISLATION ADDRESSING CYBERSECURITY AND**

**EMERGENCY PREPAREDNESS**

**MARCH 14, 2018**

**TESTIMONY OF TRISTAN VANCE, DIRECTOR,
INDIANA OFFICE OF ENERGY DEVELOPMENT;
CHIEF ENERGY OFFICER OF INDIANA,
BEFORE THE U.S. HOUSE ENERGY SUBCOMMITTEE OF THE
COMMITTEE ON ENERGY AND COMMERCE IN SUPPORT OF
LEGISLATION ADDRESSING CYBERSECURITY AND
EMERGENCY PREPAREDNESS**

**March 14, 2018**

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, I am Tristan Vance, Director of the Indiana Office of Energy Development and Chief Energy Officer of Indiana, and I am testifying on behalf of the National Association of State Energy Officials (NASEO) and our 56 governor-designated state and territory energy official members. NASEO submits this testimony in strong support of the two energy security bills and two discussion drafts being considered at today's hearing, including, H.R. 5174, Energy Emergency Leadership Act; H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act; Discussion Draft Cyber Sense Act; and Discussion Draft Enhancing Grid Security through Public-Private Partnerships Act.

We appreciate the Subcommittee's interest in and actions on the important issue of energy emergency planning, response, and risk mitigation, which was demonstrated with the passage of H.R. 3050 last year. We continue to encourage your colleagues in the U.S. Senate to act on H.R. 3050. The strengthening of state-federal cooperation on energy emergency preparedness and response through the reauthorization of appropriations for the U.S. State Energy Program and the enhanced emergency provisions contained in H.R. 3050 would significantly improve our states' and the nation's energy-related cybersecurity defenses and energy system resilience. The leadership demonstrated on both sides of the aisle on this non-partisan issue is greatly appreciated. Chairman Upton, Ranking Member Rush, Full Committee Chairman Walden,

Ranking Member Pallone, and the original sponsors of the U.S. State Energy Program (SEP) legislation and the sponsors of the appropriations Dear Colleague letter on the Program (calling for $70 million for SEP) Mr. Tonko and Mr. McKinley, all deserve special praise. We have encouraged your Senate colleagues to move the legislation quickly to strengthen our national security.

Before commenting on the bills, we would like to highlight the exceptional work of the U.S. Department of Energy (DOE) in responding to state, territory, and industry needs resulting from the historic hurricanes that devastated Texas, Florida, the Virgin Islands, and Puerto Rico, and impacted many other states last year. The support for state and federal emergency response from DOE's Office of Electricity Delivery and Energy Reliability, and resources from DOE's U.S. State Energy Program, along with collaboration among state energy directors and state utility commissioners, and the tireless efforts of the electricity, natural gas, propane, and petroleum industries saved lives and lessened economic losses by restoring energy services more quickly than would have otherwise been possible. DOE is making a difference and should be commended.

In that regard, Secretary Perry's call for the establishment of a new of Cybersecurity, Energy Security, and Emergency Response (CESER) office is precisely the type of action needed to modernize and improve our states' and the nation's ability to respond to and mitigate the risks of energy supply disruptions from all hazards. NASEO called for the creation of such an office in our bipartisan transition recommendations to the Trump Administration in early 2017. In my capacity as a NASEO Board Member, I co-chaired the NASEO Transition Task Force which

developed this important recommendation. We believe such action will have substantial life-saving and economic value to communities in every region of the country.

The Energy Emergency Leadership Act would elevate and make permanent this core DOE function, and NASEO strongly supports the subcommittee's action. We would also like to take this opportunity to point out the critical importance of making sure this new office has a well-defined and robust State Energy Security Program, adequate staff, and robust program management resources. Without a strong DOE-state energy emergency partnership, such as the one that exists today within the DOE Office of Electricity Delivery and Energy Reliability, the nation and our states will not be prepared to mitigate risks to our energy system and will not respond as effectively during emergencies. The state-federal partnership in cybersecurity and emergency response reflects the interdependent nature of state and federal roles and the new DOE CESER office should be constructed with that fact in mind. We urge you to emphasize the value of a strong State Energy Security program in the DOE CESER office.

The state-focused functions of the current DOE office supporting emergency preparedness and response (DOE's Infrastructure Security and Energy Restoration (ISER) program within the Office of Electricity Delivery and Energy Reliability) makes a tremendous and positive difference in the states' ability to deal with energy emergencies. Of particular value is the systematic sharing of data and analysis during an event.

Information sharing and coordination is at the heart of emergency response. In Indiana, for example, the propane crisis of 2013-14 resulted from a polar vortex and required a rapid response to protect the health and safety of Hoosiers who rely on propane for home heating. Additionally, we had to respond to serious concerns from our poultry industry, one of the largest in the nation, which faced the potential of losing an

entire generation of baby birds (for example, Indiana produces 73% of the nation's ducks for consumption). Baby chickens and ducks need external heat to keep warm, which is generally provided by propane-powered heating systems. Utilizing the state and federal governments' ability to connect key industry stakeholders with deployable resources, and provide information highlighting problem areas, we were able to keep Hoosiers safe and protect our economy from potentially devastating losses. Throughout this emergency, the need to further formalize cross-sector coordination and information sharing was strongly reinforced. We have heard similar feedback from every state that has dealt with energy emergencies over the past several years. While we have not faced a cybersecurity event with these types of impacts, adapting the lessons learned from these weather and market-related events to our cyber preparedness is essential.

We share the subcommittee's high-degree of concern about cybersecurity and its threat to the nation's energy system – electricity, natural gas, petroleum, and energy controls systems. State Energy Directors and utility commissioners are working with DOE, NASEO, and the National Association of Regulatory Utility Commissioners (NARUC) to identify areas of concern, share best practices, and improve information exchange with various energy industry sectors and state and federal agencies. Layering cyber-threats to the energy system (including retail customer interfaces) upon an unfolding natural disaster such as a hurricane, offers a horrific scenario. However, we must plan for, address, and prevent such possibilities. Enhancing regional coordination on energy emergency planning and exercises would be a valuable next step in this area.

For example, last month, NASEO, DOE, and the state emergency officials in the Southeastern United States held a joint workshop to improve state responses and coordination with industry during petroleum emergencies that could result from hurricanes and cyber-related events. Similarly, State-federal

cooperation on preparedness, such as the DOE-NASEO-NARUC led Liberty Eclipse energy emergency exercise conducted in December 2016 in Rhode Island, which focused on a combined cyber and natural disaster event, and the federal Clearpath exercises must continue. This is especially important given changes in personnel at the federal, state, and local levels, as well as the private sector. It would be particularly valuable to conduct smaller, low-cost regional exercises and workshops on a more regular basis. A holistic approach to regular regional exercises is essential as no two emergencies are ever identical.

The types of collaborative DOE-state-industry partnerships that improved emergency response during last year's hurricanes are emblematic of those envisioned in both the Discussion Draft Cyber Sense Act and Discussion Draft Enhancing Grid Security through Public-Private Partnerships Act. NASEO strongly supports both discussion drafts and sees tremendous opportunities for states to engage and leverage these voluntary activities with their local industry partners, DOE, and others. Cybersecurity is unlike the threats posed by natural disasters and can be overwhelming to manage. Energy system risks associated with hurricanes, tornados, flooding, earthquakes, and large-scale fires are better defined because of our past experiences and the known geographic scope of such events. Cyber threats have potentially far greater safety and economic impacts. They require multifaceted approaches and a recognition of the need to secure industry information technology infrastructure, as well as customer-owned systems that can serve as an entry point and become the "weak link" in an otherwise secure system. The discussion drafts take practical steps to address these issues and build upon the existing work of utilities, DOE, and the states.

In Indiana, we have created the Indiana Executive Council on Cybersecurity to lead a public-private partnership to enhance the cybersecurity of the state and its critical assets. The Council produces an overview

of Indiana's cybersecurity risks and opportunities, prioritizes those items by importance, and suggests and/or facilitates the implementation of projects designed to achieve the state's objectives. The council is tasked with creating and implementing a comprehensive cybersecurity plan addressing all potential cyber issues. The Council has over 250 advisory members from government (local, state, and federal), private-sector, military, research and development, and academic entities. These members serve across 20 industry-specific committees such as healthcare, finance, elections, and personal identifiable information in addition to the energy, water, and other common focuses of cybersecurity. The issues and solutions discussed in these industry-focused committees can be brought before the entire council in order to implement cross-sector response.

In addition to the Executive Council on Cybersecurity, Indiana has also started a Critical Exercise ("Crit-Ex") series. This is a state-led initiative that has both a table-top exercise and a real-world simulation to test for the penetration on a Supervisory Control and Data Acquisition ("SCADA") system of electric and water utilities. Beginning in 2016 with two federal agencies, eight state agencies, and 15 private sector organizations, the purpose is to determine government expertise on responding to cyber events, identify systemic weaknesses, determine how to protect and curtail further loss of data and functions after an intrusion, and to build partnerships between public sector agencies and the private sector.

Another innovative step to address cybersecurity in the energy sector is workforce development. Ensuring that we encourage college students to hone computer science skills and apply them to the energy sector is one way of improving our nation's security. Recently, DOE took steps to support such action through a cybersecurity contest which both engaged students in the challenges of protecting our energy infrastructure and brought together energy firms that might employ these students when they graduate. The proposed,

voluntary Cyber Sense program is likewise a practical step forward in working with the utility industry and others to continually improve our attention to thwarting cyber threats and vulnerabilities.

Equally important to our emergency response and cybersecurity activities is mitigating energy system risks in key end-use sectors. For example, many states are utilizing Energy Savings Performance Contracting and other public- private partnership infrastructure modernization approaches to upgrade energy systems at mission critical facilities and places of shelter, such as schools, police and fire stations, hospitals, assisted living facilities, fresh water and wastewater facilities, and universities, and to expand access to natural gas in underserved areas. Using cost-effective energy efficiency upgrades, on-site power options such as combined heat and power, micro-grids and distributed generation, and energy storage, as well as transmission and distribution system hardening, we have the opportunity to significantly drive down the risks to our energy system and lessen the impact of significant energy outages resulting from physical and cyber events.

Similarly, states are working with DOE's Clean Cities program to integrate natural gas, propane, and electric vehicles as a part of first responder and critical services fleets to enhance resiliency. This transportation-energy resilience initiative, called iREV, is an innovative way to reduce risk using existing funds and private sector innovation. These types of risk reduction strategies were pioneered by the State Energy Offices, DOE, utilities, and the energy industry. This is an area where modest federal support can unlock private investment.

Historic weather and non-weather energy supply disruption events such as Super Storm Sandy in 2012, the propane crisis in the winter of 2013-2014, three Colonial Pipeline events of 2016, and last year's devastating hurricanes and wild fires all required state-federal-industry mobilization to lessen the serious life, health, and economic impacts on citizens across entire regions of the

nation. During such serious energy emergencies, neither the Federal Government, nor state governments, nor the private sector can resolve these situations alone. Federal and state legal and operational authorities associated with energy emergency response require coordinated and clearly delineated actions to minimize threats to public health and safety, and to restore communities to normal economic activity.

The federal emergency response architecture established by Congress and carried out by the U.S. Department of Homeland Security with other federal agencies recognizes the critical need for direct engagement among federal, state, and local authorities in each infrastructure sector. DOE's federal leadership on Emergency Support Function 12 – Energy (ESF12) combined with state energy office and utility commission ESF12 leadership at the state level are key to addressing all threats and all hazards, improving the resilience of our mission critical facilities, and quickening the pace of energy system restoration.

NASEO sees the four bills being discussed today as a significant step forward on an urgent, non-partisan national security issue. These are problems that cannot be solved by the government or the private sector alone. We greatly appreciate the Subcommittee's continued leadership on these critical energy security issues.

Thank you for the opportunity to testify.

**Contact Information: Tristan Vance,** Director, Indiana Office of Energy Development; Chief Energy Officer, State of Indiana; 1 North Capitol Avenue, Suite 900, Indianapolis, IN 46204

***Testimony Summary of Tristan Vance, Director, Indiana Office of Energy Development; Chief Energy Officer, Indiana; Before the U.S. House Energy Subcommittee***

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, I am Tristan Vance, Director of the Indiana Office of Energy Development; Chief Energy Officer, Indiana, and I am testifying on behalf of the National Association of State Energy Officials (NASEO). Our testimony is in support of H.R. 5174, Energy Emergency Leadership Act; H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act; and discussion drafts Cyber Sense Act and Enhancing Grid Security through Public-Private Partnerships Act.

We appreciate the Subcommittee's actions on energy emergency preparedness as demonstrated by the passage of H.R. 3050 reauthorizing appropriations for the U.S. State Energy Program (SEP) and strengthening its emergency and cybersecurity provisions. Chairman Upton, Ranking Member Rush, Full Committee Chairman Walden, Ranking Member Pallone, and the original sponsors of the SEP legislation and the sponsors of the *Dear Colleague* letter calling for $70 million for SEP, Mr. Tonko and Mr. McKinley, all deserve special praise. We have encouraged your Senate colleagues to act on H.R. 3050.

First, NASEO would like to note the U.S. Department of Energy's (DOE) exceptional response to last year's hurricanes. The support for state-federal emergency response from DOE, combined with SEP resources, and collaboration among states, tribal and local governments, industry, saved lives and lessened economic losses. Secretary Perry's call for the Cybersecurity, Energy Security, and Emergency Response (CESER) office would further improve the nation's ability to respond to and mitigate the risks of energy supply disruptions from all hazards. NASEO's 2017 bipartisan recommendations to the Trump Administration called for such action. The Energy Emergency Leadership Act would elevate this core DOE function, and we strongly support the bill. We also stress the importance of CESER having a well-defined State Energy Security Program and robust program management resources. Without a strong DOE-state energy emergency partnership, such as the one that exists today, we will not be prepared and will not respond to emergencies as effectively.

State-federal coordination and data sharing is at the heart of emergency response. In Indiana, for example, the propane crisis of 2013-14 required a rapid response and government's ability to connect industry stakeholders with resources to keep Hoosiers safe and protect our local economy from potentially devastating poultry industry losses. While we have not faced a cybersecurity event with these types of impacts, we should adopt these lessons learned to our cyber preparedness. As such, we share the subcommittee's cybersecurity concerns and its threat to the energy system– electricity, natural gas, petroleum, and controls systems. Layering cyber-threats to the energy system upon an unfolding natural disaster is a horrific scenario. However, we must address such possibilities. For example, the DOE-NASEO-NARUC Liberty Eclipse emergency exercise in 2016 focused on a combined cyber and natural disaster event. These low-cost regional exercises are essential.

We strongly support the Discussion Drafts Cyber Sense Act and Enhancing Grid Security through Public-Private Partnerships Act, and believe states can leverage these activities. The drafts build upon the work of utilities, DOE, and the states. For example, in Indiana, we created the Indiana Executive Council on Cybersecurity to lead public-private partnerships, and have started a state-led exercise series focused on the SCADA systems of electric and water utilities.

Equally important is mitigating energy system risks. For example, states are utilizing public-private partnerships such as Energy Savings Performance Contracting to upgrade energy systems at mission critical facilities, and we are working with DOE's Clean Cities to add natural gas, propane, and electric vehicles in first responder fleets to enhance resiliency.

NASEO believes the four bills discussed today are a significant step forward on an urgent, non-partisan national security issue. We greatly appreciate the Subcommittee's continued leadership on these issues.

**Contact Information: Tristan Vance,** Director, Indiana Office of Energy Development; Chief Energy Officer, State of Indiana; 1 North Capitol Avenue, Suite 900, Indianapolis, IN 46204.