June 7, 2021

Submitted via email

Mr. Michael Coe
Director
Energy Resilience Division
Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8H-033
1000 Independence Avenue, SW
Washington, DC 20585

RE: Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure

Dear Director Coe:

The Solar Energy Industries Association (SEIA) is pleased to submit these comments in response to the U.S. Department of Energy's (DOE) April 20, 2021 Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure.[1] This RFI will aid DOE in developing the long-term strategy for securing the U.S. bulk power system (BPS).

Founded in 1974, SEIA is a national trade association building a comprehensive vision for the Solar+ Decade through research, education, and advocacy. We are leading the transformation to a clean energy economy, creating the framework for solar to achieve 20% of U.S. electricity generation by 2030. SEIA works with its 1,000 member companies and other strategic partners to advocate for policies that create jobs in every community and shape fair market rules that promote competition and the growth of reliable, low-cost solar power. SEIA members install solar and storage equipment throughout the country, connected both to the transmission and distribution grids. Compliance with reliability, cybersecurity, and communications standards is essential as we strive to make solar the most secure resource on the grid.

I. Introduction

We commend DOE on revoking the Prohibition Order Securing Critical Defense Facilities, which implemented Executive Order 13920 on Securing the United States Bulk

[1] The comments contained in this filing represent the position of SEIA as a trade organization on behalf of the solar industry, but do not necessarily reflect the views of any particular member with respect to any issue.

Power System[2] (BPS EO).[3] However, we also understand and appreciate the critical nature of cyber and supply chain threats, both domestic and foreign to our electricity grid. These threats cannot be ignored. DOE plays a vital role in helping the industry efforts to escalate its response to these challenges considering the immediate threats seen in recent critical infrastructure attacks. We therefore appreciate the opportunity to provide input on behalf of our members, who are key stakeholders in DOE's efforts here and in the long-term strategy for the power industry cyber and supply chain security.

With the opportunity presented by this proceeding, we first would like to highlight a few concerns in the stakeholder processes that prevents us from providing valuable input into the development of a long-term strategy towards securing the supply chain. We represent a diverse set of members from residential, commercial, and utility scale developers and suppliers who own and operate plants across the U.S. Because of our diverse interests, we have noticed that there is lack of inclusivity in the various stakeholder groups engaging with DOE, the Administration, and other intelligence agencies.

Currently, as we transition our electricity resource mix, SEIA's ability to coordinate and participate with these stakeholder groups is essential to long-term grid security. Our members have been building the future of this industry for more than a decade and are a vital partner in the development of the long-term strategy DOE is rightly looking to implement. We are committed to the President's Executive Order to secure our supply chains and safeguard any existing or new power plants to provide our grid with lasting security. However, we cannot completely fulfill this commitment without access to the collaborative initiatives or stakeholder groups which are provided the latest information sharing and solutions design coordination with entrenched stakeholders.

Solar and storage are important pillars in tackling the climate crisis. In 2020, over 20 GW of solar were installed across the U.S., with 14.3 GW coming from utility-scale projects. We anticipate that 54 GW will be installed in 2030 alone. Despite the historic growth and projections, the U.S. needs to install 270 GW of solar *above* current projections by 2030 to meet the Administration's climate goals.[4] Achieving that target will require U.S. solar capacity to reach nearly 700 GW by 2030. Renewable energy industries will play an increasingly important role in ensuring U.S. energy independence and national security. Indeed, the U.S. Department of Homeland Security (DHS) recently made clear that solar, wind, and energy storage are part of the nation's critical infrastructure.[5] And, as demonstrated during the COVID-19 pandemic, it is important

[2] Securing the United States Bulk-Power System, 85 Fed. Reg. 41,023 (July 8, 2020).

[3] SEIA explained its concerns to the Prohibition Order Securing Critical Defense Facilities in its August 24, 2020 comments.

[4] This assumes solar will make up 40% of new capacity. This is consistent with DOE's own projections.

[5] CISA Guidance on Essential Critical Infrastructure Workers, ver. 3.1, Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (May 19, 2020), available

that the U.S. have a robust and resilient domestic supply chain for critical infrastructure equipment.

It should not be overlooked that utilities provide our grid with important protections, but, as technology evolves with non-wires alternatives, flexible interconnection, and customer owned systems like rooftop solar and storage and other distributed energy resources, it is critical that these innovative companies are fully included in the development, agreement, and initiation of any new rules and regulations. The only way DOE can fully manage and assess the risk within the electricity sector, effectively secure it, and ensure resilient reliable options for the provision of service, is by harnessing the perspectives of *all* market participants.

Further, as to the long-term strategy and policy considerations informing sector specific action on cyber and supply chain security, we encourage industry and DOE to keep two fundamental considerations in mind: (1) the risks, threats, and solutions are perpetually evolving, so any action must allow for risk-based approaches with enough flexibility to adapt quickly; and (2) the electricity grid is one of the only critical infrastructure sectors which is formally regulated for cyber and supply chain security. There has been a significant investment by the power industry (including solar and storage) in the development and implementation of comprehensive cybersecurity programs, with long-term financial outlay, numerous lessons learned, and a maturity that surpasses those of other critical infrastructures. While continuous improvement must remain a priority, what is occurring in other critical sectors should only inform or impact the decision-making relative to the electricity sector where it may enhance these industry improvement efforts.

Finally, we understand the challenge of attempting to elicit both strategic input from industry while also needing specific feedback and examples to better inform how any strategy will impact stakeholders. In addition to the requested long-term strategy suggestions throughout, we have also included some specific technical examples (e.g., working toward zero-trust security) that may help DOE understand and apply the higher-level recommendations relative to our member interests. We hope these examples highlight the importance of including our stakeholders as part of these initiatives.

A. Development of a Long-Term Strategy

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

DOE is best positioned to support state, local, and tribal efforts to develop cyber and supply chain guidance and requirements to prevent the potential for a patchwork of requirements. A patchwork of requirements will become unduly burdensome, largely inefficient, and could potentially create additional security risks within industry. As independent power producers (IPPs) that typically operate across several regions of the country, our members, and most of the industry, are better served if we have a common

at:https://www.cisa.gov/sites/default/files/publications/Version_3.1_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers.pdf

security baseline to work under rather than a series of requirements representing differing state, local, and tribal interests within each jurisdiction.

Cyber and supply chain security programs are naturally designed and implemented across an organization. These organization programs bring a challenge unique to the more traditional focus by federal, state, and local agencies who focus on physical operating risks and the mitigating responses. These responses are more frequently designed to account for distinct topographies and other physical impacts unique to the location unlike organizational programs.

Today, only a few states have initiated or implemented efforts to impose local level cybersecurity and supply chain requirements, but this is beginning to change with the increased focus on cyber and supply chain threats at every level. The efforts thus far have primarily focused on addressing risks with IPPs, giving this sector a unique opportunity to understand the potential for major challenges as these frameworks expand. For example, the New York Public Service Commission (NYPSC) has set minimum requirements guidance for interconnecting to utility owner systems, as other states, like California, begin to do the same it may result in conflicting requirements and create burdensome administrative requirements across organizations operating in both jurisdictions.[6]

We commend the NYPSC, but we caution that as more states engage in individual state-led efforts that this will contribute to inconsistencies and the potential for a patchwork of requirements. If these become prevalent, and overly cumbersome and unduly discriminatory for market participants, the ultimate objective of risk-based resilient security focused programs will be severely undermined. DOE is uniquely positioned to bring states and stakeholders together to align requirements and ensure a patchwork approach does not occur as a result of well-intentioned regulators across different jurisdictions. This, along with some of the additional broader long-term strategy considerations noted below, will greatly enhance the impact DOE can have in supporting industry efforts to reach the security objectives outlined within this RFI.

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

First, as with state, local, and tribal action, it is important that DOE be engaged in the federal cyber community efforts that appear to be overlapping initiatives across the Administration and various agencies. For example, just within the last six months, President Biden issued several Executive Orders addressing cybersecurity,[7] supply chain, and critical infrastructure and the electric power system. Several Congressional bills have been introduced that attempt to expand regulation or otherwise impact critical

[6] *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, New York Public Service Commission, Case Nos. 18-M-0376 *et al.* (Oct. 17, 2019).

[7] *See* Exec. Order No. 14017, Securing America's Supply Chains (2021); and Exec. Order No. 14028, Improving the Nation's Cybersecurity (2021).

infrastructure and federal efforts related to cyber and supply chain security.[8] Meanwhile, FERC and NERC continue to focus on rulemakings and other initiatives in this space.[9] DHS (through the Transportation Security Administration) has issued a new Cybersecurity Requirements for Critical Pipeline Owners and Operators Directive[10] and is planning to issue regulation or further guidance for the pipeline industry. These efforts along with other initiatives are underway across the federal government.

Given the uncertainty and unknown impact of influence these various initiatives may have on this sector, there is a sense of upheaval within industry. The large inundation of new regulatory initiatives may impede efforts to move forward with enhanced programs if stakeholders are not confident that strong coordination is occurring. Again, DOE is uniquely positioned to lead and guide stakeholders through a risk-based approach that best fits the needs within this industry and critical infrastructure sector.

Second, we recommend that DOE lead any efforts to ensure industry-wide testing and conformity across the sector. For power systems below FERC and NERC registration requirements, e.g., distribution utilities, there is currently no commonly required standard, which leaves room for the above-mentioned patchwork of requirements to occur. For example, critical activities such as threat monitoring, ongoing audit, pen testing and incident response, all of which support strong supply chain risk mitigation, are increasingly a focus for potential regulation of assets below the BPS threshold. Regulators, led by DOE, need to better engage industry on the use of third-party services and emerging grid services providers. This cross coordination of DOE and regulators will inform federal agency and regulatory action as well as industry efforts to mature their defense posture.

Third, our industry needs better access to tools that will assist smaller entities in mitigating risk. We suggest that DOE consider providing supply chain risk management programs and supply risk scoring methodology guidance to support industry implementation efforts. Currently, well intentioned governmental and third-party actors issue guidance for addressing critical infrastructure risk to stakeholders by setting forward flexible guidelines, these guidelines often instead provide recommendations that are ambiguous and unhelpful. Industry has been a leader in building collaborative voluntary efforts to guide the implementation of internal controls. However, some SEIA members must rely on the governmental and private sector community of cyber professionals who lead these efforts, update, and inform industry on how to navigate the next threat while also being responsible for the day-to-day implementation of their own programs. The balancing of these important priorities can be overwhelming for smaller

[8] S.1400 Protecting Resources on the Electric Grid with Cybersecurity Technology (PROTECT Act) (April 28, 2021); H.R. 2980 Cybersecurity Vulnerability Remediation Act (May 4, 2021); H.R. 3138 State and Local Cybersecurity Improvement Act (May 12, 2021); H.R. 3223 CISA Cyber Exercise Act (May 13, 2021); H.R. 3243 Pipeline Security Act (May 14, 2021); H.R. 3264 Domains Critical to Homeland Security Act (May 17, 2021).

[9] *Cybersecurity Incentives*, 86 Fed. Reg. 8309 (Feb. 5, 2021).

[10] Directive issued on May 27, 2021.

entities who are often understaffed and overwhelmed by the plethora of information and threats.

To this point, the National Institute of Standards and Technology (NIST) framework should remain the industry's gold standard. The NIST framework offers consistency and a succinct guidepost for industry. This can be built upon to bring industry specific guidance and eliminate some of the ambiguity. To avoid redundancy or conflicting guidance, DOE could coordinate and integrate some of the existing industry efforts (*e.g.*, the North American Transmission Forum (NATF) and American Public Power Association (APPA) guidance materials),[11] as well as the expansive library of information already published by DHS's Cybersecurity and Infrastructure Security Agency (CISA), NIST and others. Bringing all this work together in a single guidance format may better assist industry in the development of full programs and application of additional controls to certain devices in a risk-based manner.

Further, we recommend that DOE consider leading efforts to increase industry access to CISA's threat intelligence. In addition to better real-time threat data, organizations would benefit greatly from improved approaches to distribution of the information about potential impact and recommended responsive action. For this to be successful, however, we must also focus on how to better incent suppliers to communicate with industry when a threat or intrusion has been identified. Given the diversity of the supply chain and limitations on any ability to regulate this requirement, the mandate would be implemented in the specific goods and services contracts, through inclusion of terms that suppliers report this information both to their customers and possibly to the appropriate federal agency as well. This would be an opportunity for DOE and DHS's CISA to work collaboratively on this capability with real-time access and incentivize supplier reporting. It would benefit all critical infrastructure sectors and national security.

Finally, DOE has an opportunity to improve the current approach to warnings and directives being issued and provide clearer guidance on which nation states, regional entities, and company specific suppliers pose a threat to our grid. Today, the level of uncertainty with the trading relationship with some countries, such as China (often the focus of specifically issued bulletins) coming from the federal government has created long term instability within U.S supply chains. The 2020 BPS EO created mass confusion, impacted buying and logistics decisions across the industry and had a chilling effect on security and operational activities, though this did not seem to be the objective. Lack of guidance from regulators on which equipment is safe exacerbated the challenges created by the original BPS EO. When efforts to promote enhanced security are implemented in this way, it creates a high level of uncertainty as to how industry should define security controls for their supply chains to address the threat and even where enhancements might be needed in security programs generally. DOE should seek to

[11] The APPA Cyber Supply Chain Risk Management Manual (December 2020), which was developed through a cooperative agreement with DOE public power funding (DEOE0000811) support and in coordination with the NATF Supply Chain working group initiative, specifically integrating the Risk Scoring methodology developed by that team as well as much of the other leading industry standards (CISA, NIST, DOE C2M2), available at: www.publicpower.org/resource/cybersecurity-scorecard.

improve the approach and provide better clarity and guidance, including ensuring continued stakeholder engagement in the improvements and implementation.

Our members, and all industry stakeholders, need coordinated efforts to provide consistent guidance, better access to tools, and threat awareness that aids. This coordination effort will allow industry to mitigate risks posed across the sector and specific to their own systems and corresponding supply chain risks leveraging the programs each entity has defined to meet this need. DOE is in the best position to lead this coordination across agencies of the federal government.

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

Assessing the cost-benefit implications can be challenging in this context as it can vary significantly based on the specific practice. However, in addition to the recommendations in response to question two above, we believe DOE has an important role in increasing workforce support and helping to grow the pipeline of cyber experts with knowledge of grid sector operations and challenges to facilitate better private sector practices. The cybersecurity industry has significant workforce availability issues, so the pipeline of students and career transitions for professionals needs more federal support. This could include partnerships with universities and cyber technical trade schools, small business funding focused on sector specific cyber internships and workforce development program requirements, national laboratory collaborations, and similar efforts.

4. Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

Please refer to the responses above. Coordination across all agencies and consideration of the importance of not creating additional burdensome, redundant, or conflicting requirements is critical to helping industry continue to focus on improving security programs and controls rather than directing resources to track and manage a patchwork of requirements.

B. Prohibition Authority

We do not recommend using prohibition orders to mitigate risk. From our perspective, this does little to practically address supply chain risks. In many cases, it can be an overreach with restrictions not reflective of the entity specific risk, and will ultimately cause significant, immediate upheaval of supply chains with unclear outcomes and the potential for major cost impacts across industry. The solar supply chain is diverse and starts with materials such as polysilicon, glass, lithium, polymers, steel, and aluminum. Primary finished components include solar panels, batteries, inverters, racking systems, and trackers, and a host of other related products. In 2020, 31,000 Americans were employed in U.S. solar manufacturing facilities, most of which

focus on the production of steel, racking systems, and trackers.[12] However, domestic racking and tracker manufacturers face significant hurdles from soaring commodity and logistics costs.[13]

The U.S. has enough module assembly capacity to support 7 GW of solar deployment, with most of this capacity dedicated to the residential sector products. This translates to a 13 GW shortfall based on 2020 deployment numbers. There is also little relatively domestic capacity to produce utility scale modules, e.g., bifacial modules which are increasingly becoming the preferred choice for utility scale projects. And the U.S. lacks production capacity for wafers, cells, solar glass, and many other inputs for solar modules. Moreover, there is modest capacity for inverters and other balance of system components.

While domestic polysilicon factories can support 20 GW of solar, these suppliers face an existential crisis because there are no domestic customers for their products, i.e., ingot or wafer manufacturers and U.S. polysilicon companies are effectively barred from selling into China, where nearly all ingot manufacturers are currently located.

Finally, energy storage is becoming an indispensable component of energy projects. The U.S. has an established and growing battery manufacturing base, with several facilities in place. Additional plants are announced or under construction. Domestic cell manufacturing is growing as well. However, the domestic availability of key metals for batteries, including nickel, manganese, and cobalt, is limited. Further, the domestic availability of key metals for batteries, including nickel, manganese, and cobalt, is limited.

If DOE and other agencies believe major supply chain security concerns cannot be mitigated, a long-term strategy focused on increasing domestic supply chain capabilities is the appropriate solution, not broad prohibition orders. The U.S. has a total module assembly capacity of 7 GW versus the 90 GW of solar needed in 2030. Moreover, the total amount of capacity is not the only relevant factor for utility-scale developers. Residential projects and utility-scale projects use different types of solar modules, racking, inverters, and other components. Production scale and the ability to deliver the necessary product within a limited time-period are critical issues as well. A supplier might theoretically have adequate annual capacity to fill a utility-scale order, but developers often need delivery of consistent supply over a period of a few months. This means a manufacturer must have capacity at least three to four times greater than a project. To put this in

[12] See 11th Annual National Solar Jobs Census, available at: https://www.seia.org/sites/default/files/2021-05/National-Solar-Jobs-Census-2020-FINAL.pdf.

[13] For instance, hot rolled coil prices increased over 200% between August 2020 and April 2021. See https://www.spglobal.com/platts/en/market-insights/latest-news/metals/041221-us-finished-steel-prices-expected-to-remain-high-through-september-poll. At least one solar manufacturer had withdraw forecasts due to skyrocketing commodity and logistics costs. See, e.g., https://www.globenewswire.com/news-release/2021/05/11/2227609/0/en/Array-Technologies-Inc-Reports-Financial-Results-for-the-First-Quarter-2021.html.

perspective, a developer building a 300 MW project would need to work with a manufacturer who has at least 1.2 GW of utility-scale module capacity.

In recent years, the U.S. attempted to spur domestic module and cell manufacturing through tariffs. While the Section 201 global safeguard tariffs led to some investments in module assembly capacity, such tariffs came at the cost of 62,000 U.S. jobs and 10.5 GW of solar deployment. Instead of tariffs, the entire supply chain requires significant, long-term investments to reach the necessary scale to meet the country's deployment needs.

These investments must include both supply and demand incentives. Without sufficient supply and demand certainty for domestic products, investment in manufacturing becomes too risky for investors in such a globally competitive environment. One without the other cannot sustain a strong U.S. renewable energy manufacturing base in the face of intense global competition. To that end, we recommend the U.S. government adopt a holistic approach to growing U.S. solar manufacturing which focuses on prioritizing the below policies, which will also support the specific objective here of better supply chain security within the sector:

- Creating demand certainty through a long-term extension of the solar Investment Tax Credit and increased federal procurement of domestic equipment;
- Leveraging private sector investments in new factories and equipment through a refundable manufacturing tax credit;
- Long-term support for domestic production as gaps in the U.S. solar supply are filled-in and companies scale operations; and
- A step change increase in R&D funding for renewable energy to ensure the U.S. leads the next round of solar innovation and technology commercialization.

1. To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

As noted above, we do not recommend using prohibition orders to mitigate risk. Prohibition orders and other rigid regulatory actions do not allow for the flexibility critical to adapting to the ever-changing threat landscape, nor do they consider the diversity of the stakeholders involved, including their respective risks and capabilities.

Furthermore, defense against advanced persistence threats requires significant and ongoing research and development, which can often be limited by broad prohibition orders. Creating one-off, region specific or asset restrictions to mitigate a known risk at a particular point can introduce significant uncertainty in supply chains and may incent the wrong behavior for long-term strategies by chilling innovation and encouraging a focus on this single restriction versus building strong risk mitigation programs.

Rather than issuing Prohibition Orders, DOE should support industry efforts to design supply chain risk mitigation guidance, common standards for the implementation of specific security controls from leading frameworks (e.g., NIST) and collaborative

initiatives to inform better approaches to specific principles (e.g., a robust zero trust model). If this approach were taken over blanket prohibitions, where DOE still believes a threat is significant enough to warrant restrictive measures at the level of an industry-wide action, DOE could focus on issuing enhanced mitigation requirements with clear risk mitigation guidance versus eliminating products from the supply chain.

Additionally, we reiterate our recommendations regarding supply chain security guidance and leverage of leading practice frameworks, discussed above in some detail as part of the responses to Section A. Building on those suggestions, DOE might also consider supporting efforts to provide additional common approaches and minimum baseline activities for non-BPS organization specific cybersecurity controls. These are typically implemented based on the high-level frameworks like NIST and even the DOE C2M2[14] model. These frameworks are designed to be broad domain level guidance to account for the vast differences in risk, operations, controls, capabilities, and resources of organizations leveraging them. Additional implementation guidance detail is also provided by NIST and others. However, there is still great diversity in practical interpretation and application of these controls. These differences in approach can result in unintended security gaps and challenges for cybersecurity professionals in their efforts to drive investment from internal leadership and stakeholders in proposed solutions as they often seize upon the lack of specificity in the guidance.

The NERC Critical Infrastructure Protection (CIP) Standards attempt to address this issue by including more detailed requirements and extensive guidance, which is necessary to enforceability in a regulatory scheme. The level of detail in the CIP Standards also provides helpful guidance to non-jurisdictional NERC entities. However, much of this may be more than is needed for non-BPS asset types as the risks are different and often much lower. DOE efforts to help create practical additional sector specific guidance for non-BPS assets and industry stakeholders on critical cyber and supply chain security activities (such as patching, threat management, incident response practices) could strike the right balance between the broader frameworks and detailed requirement information provided within the CIP Standards.

Finally, DOE may also play an important role in enhancing supply chain security specific to supply chain threats and commonly targeted equipment at the non-BPS and distribution level by encouraging or leading initiatives to drive adoption of common principles in industry approaches to security. The below examples illustrate this suggestion.

- **Isolated Grid Response**
  Efforts focused on expanding the lens through which threats are viewed ensuring that other threat vectors are not ignored, especially insider threats and the rise of domestic terrorism. Program and controls guidance that integrates a holistic view of an "all-hazards" approach is a better long-term strategy for resilience in security programs.

[14] The DOE issued Electricity Subsector Cybersecurity Capability Maturity Model, available at: https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

- **Zero-Trust Security Model**
  What would best serve the power industry would be encouraging all participants to move to a cyber-physical zero trust model. Zero-trust models reverse the traditional approach of essentially deferring to the assumption that everything within the corporate domain is safe and instead applies minimum security analysis and standards to everything, regardless of the origination point or assets being accessed. Driving toward this approach would directly further the goals of addressing risks with existing and installed equipment as well as enhancing overall security within any organization using this model. A zero-trust model offers an important solution to a broad set of stakeholders instead of blunt prohibitions that that address threats at a specific moment in time.

- **Incentivized Innovation and Business Integration of Security Programs**
  Prescriptive tactics fail to bridge consensus in approaches across standards and often stifle research and development. As DOE has itself recognized, incentivizing industry to move beyond compliance to a specific prohibition or set of regulations to leading practice maturity is always the better model. Identifying mechanisms to encourage and incent better security will improve mitigation of risks for specific threats more effectively than individualized prohibitions. The adoption of well-defined supply chain risk management programs will result in stronger security at every level of the organization. Further, encouraging, and even guiding, the integration of security programs as part of business models and other operational activities will also result in comprehensive security throughout organizations. Helping the industry define business revenue targets and operational metrics with a better understanding of the impact of failures to enhance approaches to security may help to accomplish this integration objective. This could assist with DOE's goal to ensure supply chain risks are adequately mitigated such that prohibition orders are rarely, if ever, needed. Aligning security incentives is vital so that power operators act in the interest of all energy consumers.

2. In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?

As noted above, we do not recommend using prohibition orders. DOE efforts to support a broader government initiative to clearly define "critical infrastructure" is needed to better understand how to identify and prioritize any such risks. The electric sector has done this initially with the designation of the BPS, robust definition of assets and thresholds that fall within it and application of regulatory requirements to specifically identify these assets (NERC CIP-002). Currently other sector "critical infrastructure" assets are not defined clearly enough to help the electric industry understand how to better support security of its own infrastructure to serve these other sectors. While industry takes steps to implement heightened security, helping these sectors more precisely understand their highest risk assets would greatly enhance the effort. DOE and NERC are natural partners to other sectors in leading this charge. Over the last decade, NERC has undertaken an extensive effort to ensure the protection of the BPS, learning many lessons in the process. The biggest of those lessons being that any initiative for other sectors must focus on clearly identifying critical infrastructure

through a robust, risk based quantitative and qualitative effort. Better defining critical infrastructure will assist all sectors, including those operating electric infrastructure supporting these sectors, in: (a) understanding and implementing robust security programs; (b) quickly responding to identified threats; (c) creating increased collaboration across critical infrastructure sectors beyond the current use of Information Security Analysis Centers (ISACs); and (d) enhancing coordination with the electric sector so our industry may better support security for our infrastructure serving these other critical infrastructures.

3. In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?

Please refer to the response to question two above.

4. Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?

Please refer to the response to question two above. Additionally, identifying and defining critical infrastructure beyond BPS would require an industry-wide initiative, much like that used to define BPS and critical cyber assets in support. SEIA again emphasizes that any initiative to define and confirm additional critical electric infrastructure should be an industry wide effort that is not exclusive to utilities. This would include the stakeholders beyond those utility interests, many of which are SEIA members that would be directly and significantly impacted by any effort. With the rise of resilient microgrids, holistic industry approaches are needed to ensure a level playing field so that all technologies and business models can compete equally, without barriers to entry to markets created by expanded security requirements.

Respectfully submitted,

/s/ Gizelle Wray

Gizelle Wray
Director of Regulatory Affairs and Counsel
Sean Gallagher
Vice President of Regulatory Affairs
John Smirnow
General Counsel and Vice President of Market Strategy
Amir Yazdi
Assistant General Counsel
Solar Energy Industries Association
1425 K St NW Ste. 1000
Washington, DC 20005
(202) 566-2873
gwray@seia.org
sgallagher@seia.org
jsmirnow@seia.org
ayazdi@seia.org