U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 14, 2022

Ms. Carla Frisch
Acting Executive Director and Principal Deputy Director
Office of Policy
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Re: Request for Information: Energy Sector Supply Chain Review; 86 FR 67695

Dear Acting Executive Director Frisch:

The U.S. Chamber of Commerce ("the Chamber") appreciates the opportunity to submit these comments in response to the Request for Information ("RFI") issued on November 18, 2021, by the Undersecretary for Science and Energy and Office of Policy, Department of Energy ("DOE").[1] The RFI, entitled "Notice of Request for Information (RFI) on Energy Sector Supply Chain Review," was issued to solicit stakeholder input regarding the supply chains of energy, energy systems and technologies, energy efficiency technologies from raw materials, processed materials, subcomponents, final products, and end-of-life material recovery and recycling.

DOE states that this inquiry is intended to support the development of an energy sector industrial base that is diverse, resilient, and competitive while meeting economic, national security, and climate objectives. More imminently, the RFI has been issued to inform the Secretary of Energy's upcoming report to the White House pursuant to that directive within Executive Order 14017 "America's Supply Chains."[2]

Consistent with the Chamber's previous comments on and communications with DOE regarding bulk electric system supply chain security, these comments leverage the broad knowledge base and real-world experiences of the Chamber's working group representing the majority of the primary participants in the electric sector supply chain for the United States bulk electric system (the "Supply Chain Working Group"). Through its interactions with other stakeholder groups, DOE, and the broader Administration, the Supply Chain Working Group intends for its efforts to supplement the contributions of an even broader set of energy sector stakeholders, many of which are also Chamber members who are likely to submit their own individualized responses to the RFI.

[1] Notice of Request for Information (RFI) on Energy Sector Supply Chain Review, 86 Fed. Reg. 67,695 (November 29, 2021).
[2] 86 Fed. Reg. 11,849 (February 24, 2021).

These comments do not intend to provide a comprehensive response to each of the fourteen topic areas identified within the RFI. The RFI's identified areas of focus include:

(1) Crosscutting topics relating to the energy sector industrial base;
(2) Solar PV Technology;
(3) Wind Energy Technology;
(4) Energy Storage Technology;
(5) Electric Grid – Transformers and HVDC;
(6) Hydropower and Pumped Storage Technology;
(7) Nuclear Energy Technology;
(8) Fuel Cells and Electrolyzers;
(9) Semiconductors;
(10) Neodymium Magnets;
(11) Platinum Group Metals and other materials used as Catalysts;
(12) Carbon Capture, Storage, and Transportation Materials;
(13) Cybersecurity and Digital Components; and
(14) Commercialization and Competitiveness.[3]

Notwithstanding the focus of these comments on the broader bulk power sector supply chain and the associated issues of concern as expressed by the Chamber's Supply Chain Working Group (focusing broadly on items 1-7 and 13 above, but with necessary overlap of the other identified technologies and components enumerated in the RFI), it is important to emphasize that each of the above topics and sub-sectors within the energy sector industrial base are not only critical to the continuing reliability and resilience of the nation's bulk power system, but are even more important in their vital role supporting the significant expansions in both transmission infrastructure and lower-carbon electric generating capacity necessary to transition the electricity sector toward a net-zero carbon emissions future. While the nation does not currently possess the commercialized technology to achieve this lofty yet laudable goal, the technologies and materials identified as subjects of the RFI will be critical – and necessary in ever-increasing quantities – to transform the energy, transportation, industrial, and other sectors of the economy to achieve longer-term climate ambition.

The Chamber has been and continues to be a strong supporter of the legislation and other policies necessary to support the research, development, and deployment of tomorrow's energy technologies, and diverse, secure, and resilient supply chains are an essential foundation to these efforts.

I. Background

The Chamber's Supply Chain Working Group has remained actively engaged with DOE on supply chain issues since the May 1, 2020, issuance of the prior administration's "Executive Order on Securing the United States Bulk-Power System" or the BPS EO.[4] That executive order declared

[3] RFI, 86 Fed. Reg. 67,696.
[4] 85 Fed. Reg. 26,595 (May 4, 2020).

a national emergency with respect to the potential for foreign entities to infiltrate and threaten the operations of the United States power grid and effectively halted the installation of bulk power system equipment "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." The BPS EO was promoted as an effort to protect against infiltration and operational threats to the U.S. power grid emanating from "foreign adversaries." However, the lack of advance stakeholder engagement and ambiguous scope of that order fomented industry uncertainty that served to halt or delay the nationwide installation, operations, and maintenance of a wide variety of critical bulk electric system equipment. This confusion occurred during a time of multi-faceted challenges, including the continued provision of reliable and affordable electric service during a pandemic and the economic and regulatory uncertainty resulting therefrom.

Following up on the BPS EO, DOE's Office of Electricity issued a July 8, 2020, "Request for Information" which solicited comment on the electric utility industry's standing practices to identify and mitigate perceived supply chain vulnerabilities.[5] The Chamber submitted a comprehensive response to the 2020 BPS RFI on August 24, 2020.[6] Rather than thoroughly considering this and other stakeholder feedback, DOE next issued its "Prohibition Order Securing Critical Defense Facilities," on December 17, 2020.[7] The Prohibition Order further exacerbated the predictable commercial and regulatory confusion generated by the BPS EO, and heightened the untenable position then imposed upon electric sector supply chain manufacturers and their utility (and industrial) customers.

Potentially issued to reduce the uncertainty propagated by the BPS EO and Prohibition Order, President Biden's Executive Order 13990, "Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis," suspended the BPS EO and, pursuant to subsequent guidance from DOE, the Prohibition Order.[8] DOE subsequently issued an order revoking the Prohibition Order,[9] and additionally issued a second request for information seeking additional stakeholder input relevant to bulk power system supply chain security.[10] The Chamber submitted a comprehensive response to that inquiry on June 7, 2021.[11]

Notwithstanding the withdrawal of the BPS EO and Prohibition Order, intervening guidance from DOE combined with reasonable due diligence activities undertaken by regulated electric utility providers continues to perpetuate ambiguity that adversely impacts bulk power system equipment and software procurement activities, thereby artificially constraining the bulk power sector supply chain. Industry stakeholders are presently working on a framework that aims to minimize the ongoing disruption to the bulk power system supply chain.

---

[5] Securing the United States Bulk-Power System, 85 Fed. Reg. 41,023 (July 8, 2020) (the "2020 BPS RFI").
[6] https://www.uschamber.com/sites/default/files/uscc_comments_on_doe_bps_eo_rfi.pdf.
[7] 86 Fed. Reg. 533 (January 6, 2021) (the "Prohibition Order").
[8] 86 Fed. Reg. 7,037 (January 25, 2021) (the "Suspension EO").
[9] Revocation of Prohibition Order Securing Critical Defense Facilities, 86 Fed. Reg. 21,308 (April 22, 2021).
[10] Notice of Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure, 86 Fed. Reg. 21,309 (April 22, 2021).
[11] https://www.uschamber.com/assets/documents/uscc_comments_on_doe_2021_bps_rfi.pdf.

II. The Breadth and Complexity of the Energy Sector Supply Chain Merits a Measured and Well-Considered Approach

From the outset, the Chamber commends DOE for the approach taken in the instant RFI, which solicits feedback from all interested stakeholders, inclusive of the supplier community, in advance of any governmental intervention. This effort stands in contrast to DOE's 2020 activities and issuances in the bulk power system supply chain space. The sweep and complexity of the bulk power system, its numerous owners and operators, and the associated global supplier/manufacturer community is significant, and unintended consequences can be many and severe if regulatory actions are undertaken without a thorough consideration of the interdependencies among the power sector, associated manufacturers, the overall national economy, and aspirational climate goals.

It is also important to recognize that securing the adequacy and resilience of the energy sector industrial base/supply chain is a marathon – not a sprint. Many small, incremental steps will be necessary to shore-up the domestic and global energy sector supply chains in a manner that provides a solid foundation for the requirements of tomorrow's energy sector. Ideally, incremental improvements will leverage existing standards, regulations, and supply chains, utilizing the guidance and authorities of existing regulators, so that the initiatives aimed at enhancing domestic supply chain security avoid unintended consequences. The questions presented in the RFI appear to recognize this delicate reality, and the Chamber encourages DOE to continue to consider the full business, technical, and policy landscapes that have built today's energy sector industrial base and that will necessarily be critical as that industrial base evolves to meet tomorrow's energy goals. However, surgical opportunities to drive supply chain enhancements in high-risk areas should be explored, especially with respect to products that may only be available from a single supplier based within a potentially adversarial nation. Federal assistance may be helpful in some of these instances where the reshoring or nearshoring of specific items is a national security imperative.

III. A Secure Energy Sector Industrial Base is a Shared Goal

The Chamber and its Supply Chain Working Group strongly support the goal of securing our nation's energy sector industrial base from all threats – physical and cyber – including those emanating from private actors or nation-states. We believe that this shared goal is best met by clearly aligning any DOE activities to fortify the requisite supply chain(s) with substantial preexisting and robust industry-led standards, including NERC CIP-013 as such is applicable to the bulk power system supply chain. Collaboration among government, domestic energy sector stakeholders, and the relevant supply chain manufacturers should be a primary focus of DOE activities moving forward.

The entirety of the Chamber's membership recognizes the critical national security importance of a domestic energy sector that is secure and resilient from sabotage, manipulation, or exploitation by nation-states or other bad actors. Moreover, these members also acknowledge – perhaps now more than ever – the critical role that supply chains play in

commerce, manufacturing, and the domestic and global economies. Just as insecure and overdrawn supply chains have handicapped the recovery of the global economy from a pandemic, supply chain shortcomings could also impair the transition of the nation's energy economy to one with less environmental impact. An unprecedented expansion of cleaner energy resources simply will not happen if the components, firmware, and software necessary for that transition are unavailable or severely limited in their supply. In addition, even if such resources are not limited in quantity, they must be of a quality that is not only resilient to natural and manmade impairments, but also secure from nation-state or other aggressor sabotage – be it physical or cyber. As such, it is essential that preexisting programs and efforts be leveraged, rather than overwritten, as DOE evaluates its available options to enhance and secure the energy sector industrial base.

The Chamber and its Supply Chain Working Group continue to strongly support the work of the Department of Homeland Security ("DHS") Information and Communications Technology ("ICT") Supply Chain Risk Management ("SCRM") Task Force and believes that task force is a valuable instrument in collaborating on the analysis and development of operational and policy recommendations for the ICT Supply Chain. As previously requested, the Chamber asks that DOE establish a task force similar to the SCRM Task Force to represent and collaborate with the electric sector (and broader energy-wide) supply chain and other energy sector stakeholders, including entities responsible for oil, natural gas, and related ICT infrastructure. For reference, members of the ICT SCRM include 40 major information technology and communications companies, along with 20 federal agencies. The ICT SCRM Task Force's four working groups relate to: (1) information sharing, (2) threat assessments, (3) qualified bidders and qualified manufacturing lists, and (4) counterfeit products. The ICT SCRM Task Force offers a useful multi-stakeholder model for coordinated industry and government supply chain risk management work – a model that could prove quite useful as DOE formulates its future supply chain enhancement activities.

The Chamber and its Supply Chain Working Group are committed to working with DOE as this process moves forward. As demonstrated by the ransomware attack on the Colonial Pipeline, energy infrastructure is critical to the functioning of our society and serves as the foundation for our economy. Heightened security standards – similar to those in place today across the electric sector – are warranted to ensure that this vital infrastructure operates reliably and is resilient to disturbances, whether natural, man-made, or otherwise. Nevertheless, DOE should weigh any energy sector supply chain initiatives against a risk-based, cost/benefit screen. This should ensure that any such actions are of reasonable scope and application. In addition, this approach should avoid an overly broad scope or outsized impact that produces upward cost impacts that undermine energy sector modernization and carbon reduction goals. Moreover, all DOE supply chain activities should be focused on minimizing stranded asset costs associated with otherwise unclear supply chain improvements.

IV. Specific Concepts Should Drive Supply Chain Improvements

The Chamber appreciates the issuance of the RFI and concurrent acknowledgement by DOE that additional stakeholder engagement is necessary to develop fully the suite of options and opportunities available to DOE and the Administration as they look to bolster the energy sector industrial base. Thoughtfully developed and clearly delineated rules, containing defined and achievable obligations, can instead support a stronger energy sector supply chain while advancing the modernization and decarbonization of our energy system.

A. Implement National Policy that is Globally Interoperable

Any new standards and/or regulations developed to enhance the energy sector industrial base should be national and uniform in nature. Certain states are experimenting with the development of their own rules and initiatives, but piecemeal and inconsistent regulation of energy sector supply chains would unavoidably be counterproductive. Energy is a national priority that does not stop at state lines, and thus state-by-state cybersecurity or supply chain standards would have little practical benefit while simultaneously imposing an inconsistent regulatory structure that would be impossible for utilities or manufacturers to manage. For example, electric sector manufacturers operating on a global scale cannot reasonably be expected to tailor domestically-bound products to fifty different sets of state-level standards. Therefore, any future DOE actions should clarify (at a minimum with respect to all facilities subject to federal jurisdiction), that nationally-applicable standards, requirements, and guidelines supersede any state entreaties to regulate within the energy sector supply chain space.

At the same time, however, DOE must recognize that the energy sector supply chain is global in nature. Some key participants essential to a strong energy sector industrial base are headquartered domestically, while others are not. Thus, nationally-applicable security standards and sourcing rules need to be globally interoperable and not force suppliers to choose between participating in the domestic market or retracting its business to other jurisdictions. In addition, energy sector industrial base policies should be crafted to avoid retaliatory policies that could disadvantage domestic supply chain manufacturers when they export their wares into other markets. Ill-conceived "localization" mandates can often invite such counterproductive trade policies emanating from outside governments.[12]

Along these lines, energy sector sourcing and security policies should seek to promote a diversity of suppliers – both domestic and international. Not only will such policies promote a robust energy sector industrial base with no single (or even dual) point of failure, but they will also prevent the development of a technology monoculture, where single technology types and sector-specific components provide a singular and identical actor vector for our adversaries, *via* cyber intrusion or otherwise.

[12] This potential friction is well-evidenced by foreign government opposition to certain local content and union labor requirements included as prerequisites for certain electric vehicle tax credits included within the Build Back Better Act passed by the U.S. House of Representatives.

B. Tailor Supply Chain Risk Management Strategy with Existing and Performance-Based Standards

DOE should focus on the development of a durable supply chain strategy that primarily leverages beneficial, preexisting supply chain risk management and security practices with select enhancements that merit the support of energy sector and supply chain stakeholders. This means that DOE's efforts to enhance the energy sector industrial base should be risk-based, with the encouragement of threat awareness and risk mitigation programs specifically tailored to guard against the associated risks and supply or resource shortfalls that they are designed to counter. The blanket avoidance of specific resources or product lines, including procurement bans based on countries of origin, can be counterproductive, as security and resource risks may take many different forms and can originate from diverse geographic locations. Further, country-of-origin prohibitions can be circumvented through transitory nations, thereby providing a false sense of security with respect to the targeted supply chain source. Instead, the adherence by energy sector supply chain stakeholders to certain controls, guidelines, and protections should alleviate the concerns attendant to supply chains sourcing from countries with otherwise questionable labor and/or cybersecurity practices.

A performance-based approach to enhancing energy sector supply chains will appropriately leverage existing standards and best practices. This approach will be the most effective mechanism to ensuring the security and resiliency of the energy sector industrial base. With respect to the bulk electric system supply chain, preexisting sector-specific efforts, such as NERC CIP-013, technical standards and reports (*e.g.*, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27402 (in development), ISO 17800, ISA/IEC 62443, NIST SP 800-53, NIST SP 800-161, NIST SP 800-82, NIST SP 800-193, NISTIR 8259A), controls, and certifications (*e.g.*, the Department of Defense Cybersecurity Maturity Model Certification), and cross-sectoral efforts such as those being led by the North American Transmission Forum, support and often mandate the adoption of supply chain best practices by bulk electric sector manufacturers and other stakeholders. Thus, as exemplified by the energy sector electricity subsector, a combination of voluntary standards and mandatory regulations facilitate a belt-and-suspenders approach to supply chain security.

C. Provide Reasonable Timeframes for Transition

Just as Rome was not built in one day, the energy sector industrial base is a complex national and global tapestry of companies large and small developed over the course of decades. Just as a small, local distributor of energy sector componentry may encounter difficulties securing alternate suppliers for specialized products, multi-national conglomerates could be forced to undertake significant realignments of supply chains and manufacturing workforces in order to adjust to new policy initiatives focused on enhancing the country's domestic energy sector industrial base. There may be instances where onshoring and/or nearshoring of certain critical manufacturing activities is prudent, but care should be taken to provide an adequate runway (*i.e.* timeframe) for such transitions.

Policies that abruptly interrupt or limit global supply chains will be counterproductive with respect to energy sector modernization and climate goals. As we have readily experienced during the emergence from the coronavirus pandemic, supply chain constraints can have both direct and indirect adverse impacts on related and even otherwise isolated sectors of the economy. Thus, while regulations or directives applicable to a specific product or country-of-origin may seem confined to the identified target(s) of such actions, other energy sector manufacturers, distributors, and critical infrastructure owners/operators will also be impacted with potential shortages and/or price increases. Across many sectors of the energy industry, these impacts are necessarily shared with energy customers comprising most of the domestic economy.[13] Therefore, it is imperative that any significant shifts in energy sector supply chain sourcing or strategy be accompanied by a minimum 2-year transition period in order to allow a smooth and managed transition for the manufacturers, suppliers, and customers of energy-related components and materials.

D. Thoughtful Consideration to Modifications in Regulatory Scope

A number of the questions presented within the RFI suggest – either expressly or impliedly – that changes in regulatory structure or scope may be necessary to expand DOE's authority over the supply chain communities for the energy sector components, both physical and digital, considered within the RFI.[14] While many energy sector critical infrastructure operators are regulated at the state and/or federal level, this current regulatory structure often aims to secure the energy sector supply chain via flow-down dictates from DOE, the Federal Energy Regulatory Commission, or otherwise. There is not necessarily a single solution here, but prudence should be taken with modifications to regulatory oversight.

This is not to say that certain changes may not be beneficial – such as when cohesive national standards could help to unify disjointed state-level mandates. Many energy sector suppliers are now subject to different compliance regimes, depending on geographic region and the practices of individual customers that interpret state or federal mandates in diverse ways. Supplier background checks differ, as do the cybersecurity requirements and certifications required of energy sector manufacturers. Therefore, if new federal standards for certain defined products serve to create a clear set of uniform national supply chain security and background check practices, well-vetted standards in this area could be beneficial so long as they support the global interoperability discussed previously herein.

However, it is important to recognize that many of the components used across the energy sector and its subsectors also have uses across other industries. Thus, the mere definition

[13] For example, in the electricity subsector many regulated utility companies provide and charge for electric service pursuant to formula rate agreements negotiated with and approved by their state utility commission(s). These rate structures intentionally provide a pass-through to customers of prudently incurred operations and maintenance costs, including any supply-chain driven increases in the cost of maintaining reliable electric service. Thus, the rushed implementation of well-intentioned long-term enhancements to the energy sector industrial base would likely have adverse short-term economywide ramifications.

[14] 86 Fed. Reg. at 67,701 (noting in one instance that "[p]roviders of digital components may not have the same supply chain security requirements as asset owners in the energy sector" and inquiring whether the government should address these perceived "gaps" in oversight and regulation).

of an "energy sector" supplier may be elusive for the purposes of scoping the reach of new regulatory mandates and directives. Moreover, many energy sector suppliers also support the critical missions of the Department of Defense, and are thereby subject to the Cybersecurity Maturity Model Certification (CMMC) requirements there. Thus, in addition to global interoperability, any scope expansion in DOE or other regulatory authority to energy sector suppliers needs to harmonize with other governmental standards already applicable to the same physical or digital components. A patchwork of diverse standards, depending upon the ultimate consumer of an otherwise identical product, would be unproductive and undermine the DOE's goal to enhance the capabilities of the energy sector industrial base to support our future energy needs.

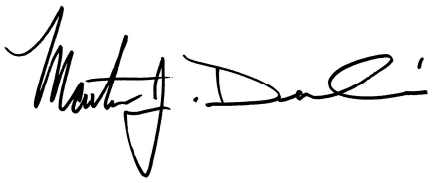
V. Conclusion

The Chamber and its Supply Chain Working Group appreciate the opportunity to provide these comments in response to the RFI. The Chamber fully supports DOE's analysis of the resources and vulnerabilities that contribute to the current state of the nation's energy sector industrial base. Given the significant investment and concomitant products and resources that will be necessary to further our energy transition, as well as maintain and operate our legacy critical energy infrastructure, it is imperative that DOE assemble a full understanding of the current state of the energy sector industrial base that can inform the development of supply chain improvements that will both support the energy transition and ensure that the nation and its energy industry are not beholden to limited and potentially compromised supplies of critical infrastructure components – both physical and digital.

The energy sector, which is predominately privately owned and operated, is critical to our national security and our everyday lives. Concomitantly, the sector's security, reliability, and resilience is essential to preserving our way of life. As such, the DOE's analysis of the numerous supply chain streams supporting this sector is important to the development of a strategic approach that insulates our energy sector from disruptions both near and far. The complexity of this sector and its associated supply chains justifies enhanced public/private collaboration to ensure that well-intentioned enhancements do not lead to unintended consequences. Starting with existing programs, procedures, and controls, and building upon them additional protections and new resource streams designed to support our energy future, will promote a secure and resilient energy sector for decades to come.

The Chamber sincerely appreciates the opportunity to comment on the RFI. If you have any questions or need additional information, please contact Heath Knakmuhs, Vice President and Policy Counsel, Global Energy Institute, at hknakmuhs@uschamber.com or Vince Voci, Director, Policy, Cyber, Intelligence, and Security Division, at vvoci@uschamber.com.

Sincerely,



Martin J. Durbin
President
Global Energy Institute

Christopher Roberti
Senior Vice President
Cyber, Intelligence, and
Supply Chain Security Policy