To: Office of Policy and Undersecretary for Science and Energy, U.S. DOE
From: The GridWise Alliance, 1800 M Street, NW, Suite 400S, Washington, DC 20036
Date: 01/14/2022
Re: RFI: Supply Chain Review (DOE-HQ-2021-0020)

The GridWise Alliance (GridWise) is pleased to submit this response to the Request for Information (RFI) seeking input from stakeholders involved in energy sector supply chain areas. GridWise commends you for soliciting stakeholder input in this regard and encourages you to continue to do so.

The mission of GridWise is to champion the principles, policies, and investments needed to transform the electricity grid by understanding the diverse perspectives and priorities of all stakeholders. Since 2003, GridWise uniquely serves the electricity industry by leveraging diverse stakeholder perspectives to articulate the numerous benefits of grid modernization. We help create a common understanding of the numerous and transformational operations-focused and policy-related changes taking place across the electricity industry. Our members include investor-owned utilities, municipal utilities, rural cooperative utilities, grid equipment manufactures and technology companies, vendors, national laboratory and research institutions, and others.

Given broad expertise along all elements and components of the grid, GridWise members are well positioned to provide insight into approaches and actions needed to build resilient supply chains for the energy sector. In advance of our responses to selected specific topic areas, we ask DOE to consider the following high-level insights on energy sector supply chains:

- The grid is in a transformational change moment. Now is the right time to foster emerging technology development and expand the U.S. energy sector industrial base to meet the demands of the transmission and distribution industries.
- New investments into both hardening and modernizing grid infrastructure are needed, and we expect these new investments to cover both traditional and innovative hardware and software technologies, as well as data analytics.
- These efforts should be conducted concurrently and supported by the U.S. government for transmission and distribution manufacturing supply chains.

In our response below, we identify the topic area and question each response relates to using the numbering convention provided in the RFI. GridWise stands ready to be a resource and looks forward to working with DOE to support building a resilient supply chain for the energy sector.

Sincerely,

Aurora Edington

Aurora Edington
Policy Director, GridWise Alliance
aedington@gridwise.org

RESPONSES BY TOPIC AREA

Topic Area 1: Crosscutting Topics Relating to the Energy Sector Industrial Base

QUESTION 1.1

How would you define the energy sector industrial base? For the purposes of informing comprehensive supply chain policies—including promoting supply chain resilience—what entities are included or not included in the energy sector industrial base?

Global adaptation to climate change is reliant on whether the global economy manages the energy transition successfully and supports capital flows to grow the supply chains needed to drive commercialization of clean energy technologies. America's energy sector industrial base (ESIB) is composed of all stakeholders that participate in the process of providing electrical products and service to the Bulk Power System ("BPS"). The functions include everything from generation, storage, transmission, voltage conversion, monitoring, maintenance, and point of service to emerging new concepts and products that could open up new markets. ESIB covers a broad group of actors that include equipment manufacturers, sub-component manufacturers, engineered product manufacturers, raw material suppliers, maintenance providers, utilities, service and repair providers, testing laboratories, and cybersecurity providers.

QUESTION 1.3

What are opportunities to expand domestic energy-related manufacturing in the United States? What conditions will lead manufacturers to reshore or expand domestic clean energy manufacturing?

Market opportunities drive manufacturing decisions especially if we focus on the current flow of capital. Industries requiring equipment-specific capitalization will require visibility on long-term, sustainable demand. This demand could be created by financial incentives to support innovative grid components that could be made domestically to help drive support for private & public DER registry platforms to enable utilities and developer "prosumers" to accelerate and integrate renewable energy resources.

QUESTION 1.5

How can policies and programs that support domestic energy manufacturing also support workforce opportunities and the creation of competitive, long-term manufacturing careers, especially for communities impacted by energy transition?

GridWise recommends you consider the following recommendations in this area: (1) manufacturing centers should be located regionally with carbon energy drawdown impacted areas; (2) educational and meaningful career transition resources must be applied prior to job loss/community impact, not after; (3) tailored career education must be part of transition technology so that it can be understood, installed, maintained, and sustained; and (4) workforce training initiative priorities should be coordinated between in-region stakeholders including local investors, educational institutions, governments, and workforce development institutions, to ensure alignment in programs objectives and regional needs.

Topic Area 4: Energy Storage Technology

Whether directly connecting to the grid as a resource, being paired with home solar panels to support system operation, or connecting to the grid as the engine in a electric vehicle, the

quantity of energy storage on the electric grid is increasing year over year. Lithium-ion (li-ion) batteries are a dominant energy storage technology today. A primary vulnerability of this technology is battery cell manufacturing and a strategic opportunity could lie in second battery life manufacturing (recycling) in the U.S. In short order, thousands of li-ion batteries from both electric vehicles and other industries will be reaching their end of life. Investment in the research of technology and production methods is needed to understand optimal ways to reuse the materials in batteries with minimal pollution.

Beyond li-ion batteries, there are a variety of other energy storage technologies both in use and under development. Other energy storage technologies include:

- other batteries (using different electrochemical technologies),
- hydrogen and its various transport/storage mediums (such as ammonia),
- thermal,
- compressed air, and
- pumped hydro.

For most of these technologies, the greatest supply chain vulnerability lies in the mining and refining of rare earth elements and critical minerals.

Hydrogen and thermal technologies may have the greatest chance of achieving long duration storage targets (>10 hours). Hydrogen has the added advantage of providing extremely long duration storage (moving energy from one season to another).

Topic Area 5: Electric Grid - Transformers and HVDC

Transformers: Grain-oriented electrical steel (GOES) is a key component of large power transformers (LPT). The lack of domestic GOES production and processing capabilities, as well as other key components, means that the US LPT industry relies on foreign supply of components and final products to fulfill US LPT demand. Government support to grow a domestic GOES industry and increase domestic supply of other components required for US LPT manufacturing will lessen domestic manufacturers' dependence on imports of foreign GOES and components, helping to ensure US manufacturing of LPTs can grow in a more self-sustaining manner. The government could support the expansion of domestic LPT manufacturing by providing tax credits and R&D support that benefits the entire LPT manufacturing supply chain. This could offset capital expenditures and workforce training costs associated with building new manufacturing facilities, and also support new LPT technology development, domestic supplier innovations, and advanced manufacturing processes. Market certainty for domestic LPT projects is an important first step that could ultimately give LPT manufacturers confidence to establish a domestic LPT supply chain.

HVDC: Demand for HVDC technology is rapidly increasing, both in and outside of the US. The global HVDC industrial base[1] is primarily concentrated in Europe so the US industry is largely

[1] The HVDC industrial base extends across a long and specialized supply chain. Leaving aside HVDC Cables, this includes, for HVDC Converters, capabilities for: production of specialized semiconductors, manufacturing of HVDC Converter equipment, assembly of HVDC Converter valve modules, manufacturing of specialized Large

dependent on foreign imports of HVDC systems. In the short term the government should focus on increasing predictability and visibility of HVDC projects in the U.S. Specific efforts could include initiation of a national development plan for HVDC projects, convening stakeholders to streamline multi-state project preparation, and supplementing private investment with federal financial support for large projects that are not financially viable based on transmission service alone. Market certainty for domestic HVDC projects is an important first step that could ultimately give HVDC manufacturers confidence to establish a domestic HVDC supply chain.

Topic Area 9: Semiconductors

QUESTION 9.1

What is the current state of U.S. and global supply chains for both conventional semiconductors used in data and sensor applications related to the energy sector and wide bandgap semiconductors used for controlling power flow in power electronics applications? What are the current and future semiconductor supply chain vulnerabilities as we scale up our efforts to transform the energy sector (energy supply, energy efficiency, demand technologies, grid, fuels, etc.) to support decarbonization? Of these vulnerabilities, which are the most crucial for the U.S. to address and focus on and why?

Crucial vulnerabilities include: (1) Shortages in semiconductors for digital components: As energy sector modernization continues, demand for semiconductors will continue to increase, driven by the digitization of previously analog equipment or devices (vehicles, protection relays, etc.). Supply will need to keep up, but experience so far indicates that supply is lagging demand. Since 2020, significant shortages in semiconductors have been observed. In this context, ensuring/improving the supply of semiconductors should be one area of focus for the government. Actions restricting the integration of certain foreign-manufactured semiconductors inside high-demand digital components to meet US grid modernization goals should also be avoided as this would significantly delay and jeopardize the delivery of such components. (2) Increasing mismatch in lifecycles: The lifecycles of semiconductor devices are growing shorter, and this is driving expensive and time-consuming re-engineering to replace unavailable or end-of-life semiconductors as well as re-certification and re-qualification of key digital components in energy sector assets that have typically long (10-20 years) lifecycles, such as protection relays or monitoring & diagnostics devices. Extending the lifecycle of semiconductors should be another area of focus for the government.

Topic Area 13: Cybersecurity and Digital Components

QUESTION 13.1

How should the government approach hardening of digital component supply chains for the energy sector industrial base against physical and virtual tampering and national security threats? How should the federal government prioritize protection of digital component supply chains?

Energy infrastructure is critical infrastructure therefore a secure energy sector industrial base is essential. The model for cybersecurity in the defense industry is the Cybersecurity Maturity Model Certification ("CMMC") framework. Today, energy sector customers are procuring

Power Transformers, construction of HVDC Converter stations, construction of Offshore HVDC Converter platforms, maintenance of HVDC Systems, HVDC Systems planning and testing capabilities, HVDC Systems engineering, and specialist engineers across this entire supply chain.

solutions that trend toward a CMMC for the energy industry, but these customer supply chain requirements are not uniform. A single standard would support greater implementation of robust cybersecurity measures. Policies that mandate greater self-assessment of cybersecurity risks by energy infrastructure owners/operators and link to global standards are necessary.

The following elements should be considered part of any federal approach:

- Generally, a performance-based approach to cybersecurity regulation, leveraging existing standards and best practices, remains a very effective mechanism to ensure the security of bulk power system (BPS) infrastructure.
- Digital components that are also substantially used outside of the BPS should not be targeted by DOE regulations pertaining to the Energy Sector Industrial Base (ESIB).
- Regulations should differentiate between code/software and the physical equipment/products that industrial control systems are made of.
- Regulations should be risk-based, and differentiate between software categories based on their scope and impact on national security: communication, encryption algorithms, general algorithms, etc.
- Regulations with impact on the supply chain of digital components should be accompanied by a transition period of a minimum of 2 years to avoid disruptions in the supply chain and enable participants in the ESIB to comply efficiently.

Some GridWise members shared examples of ongoing measures that help ensure products are resistant to physical and digital tampering, which are noted below. When considering a government approach, however, it is imperative that the burden on OEM's is not so onerous that it serves to disincentive action in this important space.

- Procuring components directly from the manufacturer or official distributors.
- Meeting current customer and project requirements with respect to the U.S. Nuclear Regulatory Commission (NRC) counterfeit, fraud and suspect items standards and related inspections and training.[2] Techniques include several methods to detect counterfeit products, including functional testing and microscopic, x-ray, x-ray fluorescence and decapsulation inspections.
- Continual testing of products throughout the procurement and manufacturing process, with processes in place for responding to and understanding performance variations.
- Asking suppliers to identify their first-tier suppliers along with key risks, mitigation strategies, and replenishment methodologies.
- Evaluation of cybersecurity components at initial supplier onboarding and with a refresher as part of the due diligence renewal every 12–18 months.
- Including in the standard purchasing terms and conditions for all suppliers Supply Chain Security and Cyber Security clauses

For critical components, an additional threat model or defense-in-depth analysis provides a foundation for understanding potential attack vectors and enables the design of compensating controls that help to mitigate potential threats from a component's weaknesses.

[2] https://www.nrc.gov/about-nrc/cfsi.html

In the case of new threats in the future, GridWise members shared some considerations. Again, when considering a government-wide approach, it is imperative that the burden on OEM's is not so onerous that it serves to disincentive action in this important space.

- Should threats arise where new authentication methods need to be developed, current practices should be revisited and product components should be redesigned. Current research is underway to enhance this redesign process; for example, building from the Trusted Computing Group frameworks, but more development, testing and evaluation is necessary before being able to offer this as standard with all new industrial products for the BPS.
- Development of a "digital twin" for supporting the protection of digital components related to information technology (IT) and operational technology (OT) components. Government investment in this type of innovative environment to deploy next generation asset management, commerce and decentralized finance solutions could lead to an end-to-end cyber physical digital asset management platform that securely digitizes intellectual property for a wide range of physical renewable energy assets and smart contract transactions. Digital twins further support new cyber-defenses, such as a "digital ghost", which uses knowledge of the associated control systems, and very advanced artificial intelligence algorithms to continuously monitor the asset's behavior. Digital Ghosts can determine if a component is behaving abnormally due to a cyberattack even when the operator's user interface says everything is OK.

QUESTION 13.2

Cyber threats to the critical infrastructure, including an explosion in Ransomware attacks, is a growing national security concern that can be enabled through digital component supply chain vulnerabilities, and there are several national initiatives underway to counter this threat. Are there energy sector-specific considerations or priorities the government should consider to support hardening of digital component supply chains against cyber threats including the use of ransomware?

Some ways to harden digital component supply chains against ransomware include:

- Developing and implementing a response plan: Utilities and vendors should have a detailed response plan for any security incidents to include descriptions of measures to address the incident and to mitigate their impact, including assessments and measures aimed at reducing the risk of re-occurrence of the applicable incident in the future. Response Plans should follow industry standard practices, currently ISO27001.
- Continuing investment in cybersecurity by government and private actors: Future technologies are likely to overcome security measures in place today. Identifying these technologies as soon as possible (quantum computing, for example) and incentivizing ESIB players in the IT and OT space to stay current in the cybersecurity space is needed.
- Looking ahead to the digital global economy and developing a framework for artificial intelligence (AI) technologies: AI chips will become the foundation of the digital global economy and embedded into every strategic U.S. industry. Considering different avenues and potentials for decentralized frameworks could reduce the risk of ransomware attacks for future technologies used on the power system.

QUESTION 13.3

What steps should the government take to improve the trustworthiness of digital components in the energy sector industrial base and reduce reliance on untrusted software suppliers, integrators, and maintenance?

GridWise members suggest the following potential steps:

- Work with industry to develop a best practices security framework throughout the supply chain incorporating the latest requirements of standards from NERC CIP/ ISO/ IEC and NIS. This framework could involve different components in various stages including: (1) during development - utilities requiring a general engineering knowledge document on product cybersecurity, a secure development lifecycle that assigns relevant security activities based on the risk level, setting minimum technical requirements related to security (e.g., no hard-coded passwords), and performing additional technical security testing; (2) during maintenance and monitoring – using a product lifecycle management tool to conduct asset management, subscribe to and participate in threat and information sharing feeds, conducting ongoing monitoring to identify vulnerabilities and support remediation actions, creating communications to alert customers of risks and provide guidance, and selecting key performance and risk indicators to evaluate product security program effectiveness; (3) during procurement – evaluating supplier product security programs, monitoring supplier product lifecycle considerations, and integrating product security into contracting terms and conditions; and (4) manufacturing – providing a validation plan for security functionalities, ensuring software and hardware authentication/certification processes, securing remote access restrictions and physical security protocols, and performing a factory acceptance test.
- Introduce policy to incentivize and accelerate the adoption of new digital component technology that simplifies ongoing complexity in the digital stack with fewer sources of truth and reduces the overall attack surface from legacy digital systems.
- Government creation of a real time software asset inventory requirement that covers all systems within the plant network and in dispatch of bulk electricity systems. This kind of visibility would give asset owners greater visibility to risk surface associated with new vulnerabilities and would improve efficiencies in software maintenance, regulatory reporting, and risk management activities. In the past, the energy sector's OT stack was marked by being relatively static and homogeneous (supplied by a small set of automation vendors). Given the nature of cloud computing, a more connected enterprise (providing plant level data to enterprise systems) and the number of IOT entrants entering the market, the security risks faced by energy companies and technology partners has changed a great deal in the past 5 years. Most energy companies do not maintain real time asset inventories of all OT. NERC CIP 002-5.1 mandates that power generators create asset inventories of critical systems, yet this inventory does not provide real time and full views of software being used within plant networks. For energy operators, the risk of not knowing software, devices, and update levels of all devices on a plant network creates significant hurdles to accurately assessing risk and responding to an event.
- Look ahead to the potential of edge computing and edge devices for real-time processing and optimization. When combined with 5G networks, edge devices allow real-time data processing to occur without needing a traditional data center. This could allow for data

processing and decision-making to occur independently without a connection, thus reducing potential cyberthreats.

QUESTION 13.4

Global digital component supply chains are highly dynamic and complex. What policies should the government pursue to illuminate provenance of digital components in energy sector systems? For example, who developed software, or hosts digital platforms, or curated data sets, and in what country? Who maintains these digital assets (if anyone) and who may have continuing access for maintenance? How should the government approach prioritizing digital components and/or systems to illuminate or examine components to manage supply chain risk?

An approach focused on the national origin of particular software components will prove both highly challenging to implement and also of dubious cybersecurity benefit. Furthermore, without bright-line rules for how to determine national origin (e.g. location where final product is manufactured, % content requirement, code authorship etc.), such an approach will not have the desired effect. U.S. firms are major exporters of BPS equipment and software worldwide, with thousands of U.S. jobs dependent on these exports. DOE should not take steps that would encourage other countries to retaliate against U.S. companies – or step back from their WTO GPA commitments.

If a regulation or policy is established pertaining to the provenance of physical digital components, it should have limitations including: (1) only applying to the provenance of the finished products, and not that of all their components and sub-components, as long as such finished products are manufactured in a trustworthy facility by suppliers who have secured their supply chains with, for instance, testing to ensure no tampering, code quality and cyber penetration checks, secured loading of firmware, etc.; (2) exempt open-source software and for information technology equipment and software with significant uses outside the bulk electric system; and (3) exempt software developed and compiled by multinational companies that are not under the control of countries of concern but whose global teams collaborating on the development of software may include some collaborators physically located in countries of concern.

Centralized storage of information pertaining to the provenance of digital components or of digital bills of materials (BOMs), especially if managed or aggregated by private sector 3rd parties, could cause substantial intellectual property issues and would lead to increased vulnerabilities in the system due to the unique door and roadmap to the system that it would constitute for malevolent actors.

QUESTION 13.6

An increasing trend in the energy sector is remote operation of systems. What policy steps should the government take to ensure the supply chain security of platforms and services used to operate critical functions in the energy sector?

Some GridWise members believe the following potential solutions are worth consideration by the government. While considering these steps, it is imperative that the government also work with stakeholders to ensure any requirements of OEM's is not so onerous that it serves to disincentive action in this important space.

- **End-to-End Encryption (E2EE).**[3] Over the last year, almost every industry has had to quickly learn how to manage a distributed workforce, with sensitive business and personal data flowing outside the traditional organizational walls. To address remote operation of systems, the energy sector should look to what other cyber-sensitive industries like finance, healthcare, and defense have adopted: E2EE, today seen as the gold standard for data security and communications privacy. The basic idea of E2EE is that sensitive data is encrypted once by the data sender into a secure 'message' that can only be decrypted by the intended data recipient(s). These encrypted messages can then be sent or stored using any arbitrary technology – secured or unsecured – because the embedded data is already encrypted. This is a technical concept called 'Zero-Knowledge' (ZN) – intermediary communication and storage components have zero knowledge about the contents of the message they are transmitting or storing. The ZN attribute of the E2EE approach is especially attractive for cloud-based distributed computing and public-internet communications as it may be difficult (or impossible) to know and trust all the potential intermediary hops waypoints or seams between two endpoints.
- **Segregation**. Platforms and services used for the remote operation of energy systems (and of other critical national infrastructure) should be segregated from public ones. Cloud and communication providers should have two separate offerings: one that is geographically limited/on-premises, and another one that is not limited/globally accessible. The government could also provide incentives to energy asset owners and operators to develop and maintain geographically/on-premises communication and platform infrastructure.
- **Global Trust Platform (GTP) pilot program**. The development of a GTP decentralized application (dApp) based upon a Zero Trust Architecture could help create a community of trust as it's not a centrally controlled system and is rooted in the principle of "never trust, always verify." A government funded pilot program could demonstrate the chain of custody for all transactions, title transfers of digital NFT assets based upon a "renewable-energy" backed currency consistent with the cornerstone of American foreign policy.

QUESTION 13.8

How can the government encourage and/or incentivize private sector owners and operators of energy sector critical infrastructure to include more national security risk considerations in their business risk decisions?

Some potential solutions include: (1) the government working with the insurance industry to create a set of criteria around risk management. Operators that met these standards would be able to realize lower cyber insurance premiums. (2) The government working with industry to support greater vocational/training opportunities in OT cyber security, such as through apprenticeship programs.

QUESTION 13.9

What specific skills are needed to develop and increase the workforce to support building, operating, and maintaining secure digital components for the energy sector industrial base? For example, is there a skills gap and/or supply gap in the workforce that develops and maintains software for industrial control systems? Of those skills, which ones are lacking in current education/training programs? What resources (including time) and structures would be needed to train the cybersecurity workforce? What worker groups, secondary education facilities, and other stakeholders could be valuable partners in these training activities? What new education programs should be included (developed?) to prepare the workforce?

[3] The following concept whitepaper outlines the potential use of E2EE in the utility industry: https://www.bettergrids.org/opencip-concept-whitepaper

Consider providing support and funding for vocational programs like the CIISA program, cyber security training for suppliers/vendors and utilities, mandatory network and communication training for energy sector personnel, compulsory courses in cyber security for energy related programs

QUESTION 13.10

What other input the should the federal government be aware of to support a resilient supply chain of cybersecurity and digital components?

Consider hosting more incident response and training exercises for energy and critical infrastructure providers, encouraging information sharing through ISAC engagement, and working closely with technology providers to address security throughout product and service lifecycles.

Topic Area 14: Commercialization and Competitiveness

QUESTION 14.1

What data, methodologies, and metrics can help assess current and future competitive advantages for clean energy technologies?

Some metrics that could help assessment include: (1) metrics or data that shows competitive advantages for cost per MW hour delivery; (2) total life cycle generation versus life cycle costs; and (3) total carbon reduction (all component materials) per KWH compared to non-green energy. Some GridWise members also believe that methodologies & data must exclude subsidies or government assistance to ensure the analysis is a 1-to-1 comparison of the future competitive advantage.

QUESTION 14.2

What existing economic and market analysis do you rely on to assess current and projected technology market demand?

Examples of analysis GridWise members use to assess the market include: (1) reports from industry analysts such as Gartner, Forrester, etc.; (2) first-person research commissioned around specific technology concepts; and (3) leveraging past customer sales to provide a basis for comparison where projected growth of sales can be based on peer-reviewed on market research, customer feedback and market need assessment.

QUESTION 14.10

How do U.S. trade policies impact the commercialization and competitiveness of clean technologies in the U.S.? Where might changes to trade policy positively impact U.S. competitiveness in clean tech sectors?

Many clean technologies manufactured in the U.S. rely on components that are cost-effectively sourced globally, absent barriers to trade imposed by the government (e.g. tariffs and quotas). Tariffs on steel and aluminum imports, as well as on a wide swath of imports from China, are in fact tariffs on products that are used as components of U.S.-made clean technology. Many of these technologies are not abundantly available or are completely unavailable from a domestic producer. Tariffs on such components raise the cost of domestic production of clean technologies and make U.S. clean technology less competitive vs. foreign competition, whose fully assembled

products (whose components are not impacted by U.S. tariffs) enter the U.S. tariff free. This also raises prices on consumers, slowing adoption of clean technology.

Wider access to cost-effective domestic components would be welcomed by the U.S. clean tech sector - from semiconductors to neodymium magnets to metals. But tariffs do not guarantee that such increased domestic supply will appear. In the meantime, such a "stick" approach punishes the U.S. clean tech sector by raising the cost of its components and making it less competitive with foreign competition. Rather, the government should pursue policies that positively promote U.S. manufacturing capacity of key components with policy "carrots" focused on the would-be domestic component manufacturers.

GridWise strongly supports the Advanced Manufacturing Tax Credits, to support the development of U.S. clean energy equipment factories, and more widely-applied production tax credits similar to what is included in the Build Back Better Act introduced in the 117th Congress. The Section 48C Advanced Manufacturing Tax Credit in ARRA originally provided a 30 percent investment tax credit to 183 domestic clean energy manufacturing facilities valued at $2.3 billion and was extended to provide an additional $150 million in 2013. The tax credit helped build a U.S. manufacturing capacity and supported significant growth in U.S. exports. Qualifying manufactured clean energy products in the statute include electric grid to support the transmission of renewable energy, including storage.

USG support for the energy sector industrial base must be provided broadly and deeply across the domestic supplier base, not just the final assembly of energy equipment in U.S. factories. It is important that the USG design tax credits that are compliant with the WTO Agreement on Subsidies and Countervailing Measures ("SCM Agreement"). This can be achieved either by implementing policies that either A) are designed to be extremely broad-based, applied objectively to a wide array of industries, and minimize distortions to international trade, or B) update the SCM Agreement's rules to allow more subsidies to support the U.S. and global energy sector industrial base.

QUESTION 14.11

What new and innovative actions can the government take to encourage commercialization of U.S. innovation and increase U.S. competitiveness?

One innovative action that the government could consider is the development of a Global Trust Platform (GTP) decentralized application (dApp) based upon a Zero Trust Architecture and an intelligent digital twin asset economy. The GTP could reduce friction, counterfeit, fraud, lower fees, and increase efficiencies for government agencies, business, and consumer services.