UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Request for Information (RFI) on Ensuring the)
Continued Security of the United States Critical)
Electric Infrastructure)

VIA EMAIL
ElectricSystemEO@hq.Department.gov

COMMENTS OF FORTRESS INFORMATION SECURITY AND ITS SUBSIDIARY CYBER RISK UTILITY, LLC D/B/A ASSET TO VENDOR NETWORK ("A2V")

1. ABOUT RESPONDENT

Fortress Information Security, together with its subsidiary Cyber Risk Utility, LLC (d/b/a the "Asset to Vendor Network or "A2V" or "Fortress") provides cyber supply chain risk management solutions, and our mission is to secure critical infrastructure by managing cyber supply chain risks from vendors to assets. Fortress specializes in Utilities, the Department of Defense, the Department of Homeland Security, and their critical suppliers.

This remainder of this section is referred to as "Our Solutions" or "Cyber Supply Chain Risk Management Solutions ("C-SCRM")."

In pursuit of our mission, Fortress delivers four capabilities: (1) proprietary software known as the Fortress Platform, (2) an information sharing exchange known as A2V, (3) vendor and product risk tools, data, and analytics such as the Related Entity Discovery methodology ("RED") and File Integrity Application ("FIA"), and (4) a variety of managed services to help our clients produce results. The Fortress Platform enables cyber supply chain risk management program execution and maturity. The A2V information sharing network is the only central repository focused exclusively on the unique needs of the Utility Industry and its critical suppliers. Finally, Fortress correlates dozens of data sources and its cadre of research analysts and engineers conduct comprehensive monitoring and data-driven solutions, which cover cybersecurity, FOCI, components, and other risks.

2. RESPONDENT'S EXPERIENCE

This section is collectively known as "Our Work" or "Fortress' Experience."

Fortress provides Cyber Supply Chain Risk Management Solutions to investor-owned utilities ("IOUs"), regional transmission organizations ("RTOs"), Public Utilities, Utility Cooperatives, and their critical suppliers.[1] In total, it is our privilege to serve over 100 energy companies, subsidiaries and their critical suppliers, employing over 250,000 employees (about half the population of Wyoming), providing energy to over 50 million people (about twice the population of Texas) in the lower 48 states. We manage the cyber risk on over 40,000 vendors and 300,000 assets for our clients. We established the A2V network in partnership with American Electric Power ("AEP") and Southern Company ("Southern").[2] The A2V network is a central repository used by our clients and over a hundred of their most critical suppliers driving security and trust through transparency. AEP, Southern and Fortress understand the prohibitive cost of cyber securing the supply chain, and so, A2V has been patterned after the success in the financial industry to drive maturity and reduce compliance costs. It is estimated that A2V can

[1] We also provide cyber supply chain risk management solutions to the DOD and DHS.

[2] ASSET TO VENDOR, https://assettovendor.com/ (last visited June 7, 2021).

save the industry $8 billion (about $25 per person in the US) in compliance costs in the first five years excluding the business benefits and risk reduction.[3]

We operationalize clients' compliance with the North American Electric Reliability Corporation's ("NERC") Critical Infrastructure Protection ("CIP") reliability standards.[4] We also operationalize our clients' cyber supply chain security programs using recognized frameworks, such as that of National Institute of Standards and Technology ("NIST") for Improving Critical Infrastructure Cybersecurity.

At Fortress, we see different maturity levels in our clients' (both asset owners and their critical suppliers) cyber supply chain programs. The A2V network drives maturity by easing expertise and financial constraints on less resourced asset owners and suppliers. Instead of each utility company completing its own supply chain risk assessment, we complete the risk assessment and share congruent information to simplify what otherwise would be a redundant, costly, and burdensome process for asset owners and their suppliers. Thus, a central repository like A2V increases cyber supply chain maturity by sharing information, driving best practices, and reducing compliance costs to all those involved, particularly less resourced asset owners, suppliers, and other stakeholders such as State and local governments and Indian Tribes.

The industry's central repository, A2V, that Fortress operates, contains information on 20,000 vendors and products. We monitor these vendors' and products' security controls, vulnerabilities, FOCI, and breaches. We have completed tens of thousands of assessments of vendors and products just in the last year. These assessment include validated vendor control

[3] Fortress supplied detailed calculations of these savings as part of its response to the Department's RFI in September 2020.

[4] See, e.g., North American Elec. Reliability Corp. [NERC], Cyber Security – Supply Chain Risk Management, CIP-013-1, (2021), https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

assessments, any-source vendor assessments, any-source product assessments, product teardowns, software Bill of Materials ("SBOM") assessments, hardware Bill of Materials ("HBOM") assessments, FOCI assessments ("RED"), and File Integrity Assessments ("FIA").

The first step to long-term successful cybersecurity requires full C-SCRM program maturity and resources to achieve the requisite maturity. Our Work has taught us that while asset owners and their suppliers have expended tremendous effort and resources to implement C-SCRM programs, many as recently as the last year, much more maturation needs to take place to cyber secure our supply chain. There is little time as the threat is upon us.[5] Collaboration and support between the private sector and governmentat all levels, the utility industry, and the cybersecurity industry, will facilitate achieving full maturity, and subsequently, successful cybersecurity. We accelerate achieving C-SCRM program maturity by removing duplicative, inefficient work on behalf of every industry participant involved.

3. OPENING COMMENTS

In this Request for Information ("RFI") by the Department of Energy ("Department"), one underlying question to be determined is whether a Prohibition Order will be effective in securing the U.S. critical infrastructure, or whether some alternative will be more feasible. Private companies in the energy sector currently implement a risk-based approach to securing their critical infrastructure against cyberattacks. To serve the purpose of this RFI, it is important to consider the merits and the demerits of a Prohibition Order against those of a risk-based approach, which we recommend as an alternative.

[5] See, e.g., SOLARWINDS, https://www.solarwinds.com/sa-overview/securityadvisory (last updated Apr. 6, 2021, 9:00 AM); Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, WALL ST. J., https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 (last updated May 19, 2021, 4:51 PM).

A Prohibition Order, which includes the process of creating a list of equipment that cannot be imported is problematic.[6] In creating such an order, it will be difficult to concisely define which equipment *and their component parts* [emphasis added] are subject to this Prohibition Order without being overinclusive or underinclusive. The most likely case here is that the Prohibition Order will be overinclusive. This will in turn lead to hardship for utility companies in procuring equipment necessary to provide critical infrastructure. Executive Order 13920 shows how vague Prohibition Orders tend to be, and the effects of a vague Prohibition Order.[7] Executive Order 13920 merely stated that it controlled "any bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[8] This order turned out to be too broad and left industry participants scrambling to decipher which specific equipment and their components were included and which were not.

However, as recent attacks on critical vendors such as MicroSoft,[9] SolarWinds and Colonial Pipeline remind us, much more needs to be done, so the temptation to implement tools such as Prohibition Orders is understandable. Based on Our Work, a more suitable alternative to the Prohibition Order is strengthening the presently used risk-based approach reflected in the NERC CIP standards. With this, companies are given the opportunity to identify and strengthen weak points. According to *McKinsey & Company*, the risk-based approach "designates risk

[6] Josh Fruhlinger, Whitelisting Explained: How it Works and Where it Fits in a Security Program, CSO Online, Jun. 17, 2020, https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

[7] Executive Order on Securing the United States Bulk-Power System, The White House, May 1, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

[8] Id.

[9] Kate Conger and Sheera Frenkel, Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China, NY TIMES (Mar. 6, 2021), https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.

reduction as its primary goal" and "distills top management's risk-reduction targets into precise, pragmatic implementation programs with clear alignment from the board to the frontline."[10] Our recommendation is in line with the *McKinsey & Company* explanation that "a company will no longer 'build the control everywhere'; rather, the focus will be on building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats—those that target the business's most critical areas."[11] A risk-based approach will therefore give companies more autonomy in determining which aspects of their operations are more susceptible to cyberattacks. Currently, CIP standards are used in risk management procedures. By their very nature, the CIP standards are a risk-based approach as they set the minimal requirements for companies to follow and allows them to decide how best to satisfy those requirements. Unlike the Prohibition Order, a risk-based approach is neither underinclusive nor overinclusive. Rather than introducing new Prohibition Orders, we recommend that the Department strengthen and support the risk-based approach in place and enhance it to better secure the continued security of the U.S. critical infrastructure.

As we proposed in "Cyber Securing America's Bulk Power Systems - a Public Private Partnership ("CABAP")," [12] rather than having either the public or private sector solely manage cybersecurity, we recommend that the Department implement a public-private partnership like the proposed partnership in NIST SP 800-161 Rev.1.[13] Public-private partnerships are not a novel innovation but have been used in the United States since 2010 with much success in

[10] Jim Boehm et al., The Risk-Based Approach to Cybersecurity, McKinsey & Company, Oct. 8, 2019, https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity.
[11] Id.
[12] Submitted to John N. Augustine on January 20, 2021 Unsolicited Proposal Manager, U.S. Department of Energy, doeusp@netl.doe.gov
[13] Draft NIST SP 800-161 Rev. 1, Cyber Supply Risk Management Practices for Systems and Organizations, 19

different sectors to develop infrastructure.[14] In adopting public-private partnerships as we recommend, the private sector can contribute its business, technogy and risk management expertise and the government can supplement the private sector's current efforts by providing subsidies to companies with lesser resources to empower them to enhance the necessary security precautions. We also recommend that the government increase its intelligence-sharing efforts to give the private sector access to the information necessary to implement efficient procedures.

4. INFORMATION REQUESTED

a. Response to Section A. Development of a Long-Term Strategy

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

Fortress' Experience in delivering C-SCRM Solutions is that technical cyber talent is scarce. The International Information System Security Certification Consortium ("(ISC)^2"), a non-profit organization, reported that the global cybersecurity workforce gap stands at 3.1 million as of the end of 2020. They estimated that the size of the United States' workforce gap at 359,236 in as of the end 2019. Among other costs, the cost and scarcity of cyber talent and strained utility budgets demand a cost-efficient approach to cybersecurity. Coordination between the private and public sector will decrease the demand by eliminating redundancy as electric infrastructure could simply share their security data with one another. The States, Indian Tribes, and local governmentmust share information, and they must have a reliable method to share that information.

[14] "The history of the P3 market and what's next," NMBL Strategies, Fen. 24, 2021, https://www.nmblstrategies.com/blog/the-history-of-the-p3-market-and-whats-next.

Additionally, State, Tribal, and local governments would enhance their security efforts by continuing to support the growth of the cybersecurity talent pool. The States, Indian Tribes, and units of local governmentneed cooperation from both utility companies and the cybersecurity industry to enhance their security efforts in securing the electric grid. Also, response to cybersecurity threats should be rapid, and given the size of the utility industry, creating a central repository would best achieve these goals.

ii. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure, 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?

Fortress' Experience in delivering C-SCRM Solutions particularly in response to CIP-010-3 and CIP-013-1 has given us insight into this question. As a result of Our Work, we have the following recommendations:

1. Accelerate the maturity and alignment of cyber supply chain risk management programs through standardization and investment, and
2. Facilitate the sharing of threat and breach information.

We recognize that a significant contributor to the financial sector's success is the time it has had to mature over the last 15 years. Since the energy sector Departments not have the time necessary to mature as the financial sector did, it is essential that our sector accelerate this maturity. Such acceleration can be achieved through (1) adoption of standards, (2) (3) adoption of a central repository, and (4) grants and subsidies for companies to bolster risk management efforts of the less resourced entities. First, Our Work has taught us that we need standards. We support the efforts of the North American Transmision Forum to standardize vendor control criteria questionnaires and the Idaho National Laboratory's Consequence-driven Cyber-informed Engineering ("CCE"). Adoption of standards includes facilitating and mapping suppliers' select standard third party certifications[15]. Second, designating an operational central repository, such as A2V, will reduce the effort to execute current cyber supply chain risk management programs so that scarce resources can be re-directed to maturing cyber supply chain risk management programs. Third, the Federal Governments should allocate critical infrastructure grants to help accelerate the maturity of smaller asset owners and critical suppliers. There is significant precedent for this. For example, consider the federal government's grants for maritime cybersecurity and general preparedness.[16]

To further strengthen the cybersecurity of the U.S.'s critical infrastructure, it will be invaluable to share information on breaches and potential high-risk discoveries with other companies so all companies can work to strengthen their risk management procedures. This incident information sharing also comes with its own merits and demerits—the right of asset owners and their suppliers to keep their information private versus the right to privacy. Although mandating total transparency will benefit America as a whole, conflicts with our long-held traditions along with private companies' desire to keep their business private will cause them to

[15] ISO, SOC, CMMC, etc.

[16] See eg. Port Security Grant Program, ABS Group, https://www.abs-group.com/What-We-Do/Safety-Risk-and-Compliance/Cybersecurity/Maritime-Cybersecurity/Ports-and-Terminals/Port-Security-Grant-Program-PSGP/, ("The program provides funds to state, territorial, local and private sector partners to support increased port-wide risk management"); DHS Announces Funding Opportunity for $1.87Billion in Preparedness Grants, Department of Homeland Security, (Feb. 25, 2021), https://www.dhs.gov/news/2021/02/25/dhs-announces-funding-opportunity-187-billion-preparedness-grants, ("Grant recipients under the State Homeland Security Program and Urban Area Security Initiative will be required to dedicate a minimum of 30% of awards to address these five priority areas: cybersecurity (7.5%, an increase of at least $25 million across the country); soft target and crowded places (5%); information and intelligence sharing (5%); domestic violent extremism (7.5%); and emerging threats (5%).")

push back. To resolve this conflict, we recommend that regulators work with the private sector to agree on a limiting principle on this information sharing mandate.

In addition to the private sector's desire to keep its workings private, it also struggles to adopt efficient measures due to the inaccessibility of vital information that is usually classified. Given that asset owners and their suppliers are under attack from sophisticated nation state threat actors, we would recommend that classified information be separated from non-classified information to the furthest extent possible so that the private sector can access more information with which to secure itself without threatening national security.

iii. *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?*

Our Work in delivering C-SCRM Solutions particularly in response to CIP-10-3, CIP-013, Executive Order 13971, and Section 889 of the National Defense Authorization Act ("NDAA") result in the following recommendations in addition to those delineated in the foregoing question. Our recommendation is to strengthen and support existing regulations to mature, and create consistency between, the industry's cyber supply chain risk management programs.

The resource differential between large and small asset owners and small and large suppliers leads to the larger entities implementing more mature risk management programs, as opposed to smaller entities that often have limited resources. Currently, BES procurements are governed by CIP-013 among other standards, which provides baseline requirements to companies for risk management. CIP-013's requirement to implement supply chain risk management plans has served its purpose albeit at varying levels of sophistications and therefore effectiveness. To continue the progress started by NERC under CIP-010-3 and CIP-013, we recommend that the Department work with NERC on strengthening existing standard risk management plans to have the following minimum requirements:

1. Expand scope from medium and high-risk BES to other procurements deemed to impact the BES,[17]
2. The architecture and composition of high-risk OT and IT products procured should be assessed considering the asset owner's deployment,
3. Consideration of FOCI into high-risk procurements (see also question "iv." below),[18] and
4. Once procurement is complete, high-risk vendors and products should be continuously monitored.

The above, combined with the recommendations in the foregoing question, would serve to inform utility procurement policies as vendors would be practically required to provide all information that is relevant to perform cybersecurity assessments.

iv. 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?

Based on Our Work conducting FOCI risk assessments[19] to help our clients make procurement decisions, we experience two challenges: (1) availability of information to evaluate

[17] The Office of the Comptroller of the Currency (OCC) mandates banks to "practice effective risk management" These risk management processes are expected to be proportional to the level of risk that each bank faces. Rather than implement one set standard for all banks, the OCC mandates banks to implement a more rigorous oversight for critical activities "or other activities that could cause a bank to face significant risk."

[18] Due to the uncertain regulatory environment, few utilities have developed programs to assess FOCI risks in the component and subcomponents supplied by their vendors. However, the lack of specificity as to criteria that places a vendor under FOCI creates problems for the cybersecurity industry, utilities, and vendors alike.

[19] Fortress evaluates physical, manufacturing, and cyber presence of our client's supply chain in foreign jurisdictions. We also consider vendor corporate hierarchy and any Merger & Acquisition data for FOCI risks. Additionally, we consider foreign ownership data as well.

"ownership, control, and influence" (particularly with private companies), and (2) the definition of "ownership, control, and influence."

Fortress' Experience is that gathering accurate data on public companies was easier than finding data on private companies and that the most reliable method to obtaining data relevant to FOCI risks is to obtain the information directly from the vendor under consideration. Although the largest product company in the world publicly discloses their supply data, private companies tend to guard their data.[20] Strengthening existing supply chain risk management standards that mandate disclosure of supply chain data (or a certification as recommended below) from suppliers will enhance the effectiveness of existing FOCI assessments. For example, entities must complete and keep a SF 328 updated to obtain access to classified information.[21] Additionally, it is Fortress' Experience that many of these suppliers also serve the Federal Government, so it will be easier for them to provide the requested information.

Our Work shows that the lack of a formal definition for "ownership, control and influence" in the current FOCI regulation results in unpredictable and inconsistent FOCI assessments. In our experience, a proper FOCI assessment includes the review of private corporate documents detailing a myriad of extraordinarily complex corporate structures such as veto rights, voting rights just to name two. One model for conducting this complex evaluation at scale is the National Minority Supplier Development Council ("NMSDC") that certifies Minority Business Enterprises' ("MBEs") eligibility for governmentset asides when minorities own [control or influence] at least 51% of the contract recipient. This program has matured over many

[20] APPLE, https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf (last visited June 7, 2021).
[21] Foreign Ownership, Control, or Influence (FOCI), 32 C.F.R. § 117.11(c) (2021).

years to prevent abuse, which is perpetrated through opaqueness and complexity.[22] Under this program, independent assessors review applications including corporate structure documentation and provide a certification of MBE. Our recommendation to the Department is to call for the certification of the level of "[Foreign] ownership, control and influence" using a model like that of NMSDC. The Department could cause this certification to be securely distributed through the central repository recommended above.

Alternatively, the Department might consider that the United States Nuclear Regulatory Commission ("NRC") was faced with a similar dilemma when it came to the import and export of nuclear materials. Rather than issuing a Prohibition Order, the NRC opted for a risk-based model.[23] With this model, the NRC has identified ten restricted countries[24] to which export of certain materials requires the "issuance of a specific license by the NRC including Executive Branch review pursuant to § 110.41."[25] The NRC has not issued a blanket ban on any material or any country, but it has been successful in ***regulating*** how materials are exported. The NRC has listed certain conditions under which an exporter will need a special license conditioned on the Executive branch providing "judgment as to whether the proposed export would be inimical to the common defense and security, along with supporting rationale and information."[26]

b. *Prohibition Authority*

i. *To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on*

[22] NMSDC's program includes the following definition, for publicly owned businesses, for ownership: "at least 51% of the stock is owned by one or more minority group members." NMSDC, https://nmsdc.org/mbes/mbe-certification/ (last visited June 5, 2021).
[23] Export and Import of Nuclear Equipment and Material, 10 C.F.R. § 110 (2021), https://www.nrc.gov/reading-rm/doc-collections/cfr/part110/full-text.html.
[24] §110.29
[25] §110.2 "Restricted Destinations"
[26] §110.41(b)(1)

parts of the electric distribution system, i.e., distribution equipment and facilities?

Although the Department could issue Prohibition Orders, it would be more advisable to strengthen and support the risk-based approach we currently have since it is familiar, and we better understand how to execute it. As outlined above, although Prohibition Orders come with certain benefits, they also come with demerits. Blanket Prohibition Orders cost utilities significantly more since the equipment needed is currently imported at lower prices than we could purchase from American suppliers, if available. Strengthening and supporting the risk-based approach with standards and a central repository will benefit the industry and particularly smaller utilities and suppliers who typically lack the resources to implement risk management procedures. Although most of America is served by larger utilities, a sizable portion is served by smaller ones.[27] Given that the aim of the Department is to fully secure critical infrastructure, it would not be advisable to secure a portion of companies that provide critical infrastructure while leaving the other part susceptible to attacks.

ii. In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action

Based on Our Work, the Secretary should not pursue a Prohibition Order and instead seek to strengthen and support the industry's risk-based approach elucidated above. Regardless of the approach taken, the Secretary should seek to secure electric infrastructure serving other critical infrastructure sectors. Cybersecurity defense depends on depth. Adverse actors will target the

[27] In 2019, 57% of electricity was sold by IOUs, 16% by Public and Federal Entities, 12% by Cooperatives, and 16% by Other Providers. U.S. Energy Information Administration, Electricity Explained: Electricity Generation, Capacity, and Sales in the United States, https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php (last updated Mar. 18, 2021).

weakest, least-secured link to compromise critical infrastructure. Therefore, we must secure all critical infrastructure. Implementing a risk-based approach to provide structure and clarity to industries' cybersecurity initiatives will preserve flexibility in securing critical infrastructure, without compromising autonomy of those various industries.

iii. 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?

The response to question II.2 is also applicable to electric infrastructure that enables national critical functions.

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

Our Solutions help utilities identify and manage IT and OT Bulk Electric Systems ("BES") including software patches and configurations for those systems. Fortress' Experience is that utilities can identify critical infrastructure within their service areas that either they or regulations have identified high-risk. However, Our Work around the NDAA Section 889 requirement's, EOs and CIP standards also show that identifying hardware and software components (i.e., HBOM and SBOM) is a new and challenging requirement that necessitates cooperation between asset owners and suppliers, especially considering our objective to accelerate cyber supply chain maturity. As previously written, a public-private partnership together with standardization and utilization of a central repository will accelerate maturity in this area and enhance access to these resources to smaller asset owners and suppliers.

5. CLOSING COMMENTS

The energy sector is a key stakeholder in America's cleaner sustainable future.[28] To enable this future, the energy industry is leading a digital transformation and an electrification of our economy. This progress, however, comes with considerable cyber risk that our adversaries are clearly intending to exploit. It is therefore essential that the United States strengthen its critical infrastructure cyber defenses including that of its vast supply chain. This must be done as quickly as possible. The good news is that the private utility industry, comprised of asset owners and their suppliers, as supported by government at all levels are building and maturing supply chain cyber security programs. Recent attacks highlight that more needs to be done and faster.

Based on Our Work providing C-SCRM Solutions to asset owners and critical suppliers, we observe that the sophistication of cyber supply chain security programs is inconsistent, and therefore, some programs are more effective than others. This is a predictable outcome considering the scarcity of cyber security talent and disparity of resources between large and small entities. To mitigate this, we recommend:

(1) strengthening and supporting current regulations to effectively create a higher bar,
(2) reducing the burden of compliance by (i) adopting standards such as those published by the North American Transmission Forum and the Idaho National Laboratory and (ii) utilizing an operational central repository such as A2V to avoid waste and duplication and enable reallocation of scare resources to higher effectiveness activities, and
(3) providing less resourced asset owners and suppliers financial assistance to secure themselves.

As citizens and stakeholders, we must work together to cyber secure our nations and planet's future.

[28] Molly Whalton, If the Energy Sector Is to Tackle Climate Change, It Must Also Think About Water, International Energy Agency (Mar. 23, 2020), https://www.iea.org/commentaries/if-the-energy-sector-is-to-tackle-climate-change-it-must-also-think-about-water.