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

Via: Electronic Submission

 *ElectricSystemEO@hq.doe.gov*

Date Submitted: June 7, 2021

From: **1) Mr. Dominick Birolin**

 Vice President of Cybersecurity Services

 **PFES**

800 Hillgrove Avenue, Suite 201

Western Springs, IL 60558

 dbirolin@pfes.com, 910-660-3204

 **2) Mr. Patrick C. Miller**

 President

 **Ampere Industrial Security**

 1631 North East Broadway #752 Portland 97232

pmiller@amperesec.com, 503-272-1414

 **3) Ms. Larisa Breton**

 President

 **FullCircle Communications, LLC**

 32406 Franklin Road
Unit 250344
Franklin, MI 48025

 larisa@fullcirclestrategicsolutions.com

 (248) 635-5699

*The remainder of this title page is intentionally left blank.*

Dear Director Coe:

Thank you for this opportunity to respectfully present inputs to your Request for Information. As President Biden stated in his Address to Congress on April 28, 2021, it is time to solidify national energy infrastructure. With a combined 50+ years in cybersecurity policy, incident response, and auditing in Federal, Regional and private-sector roles, we know a comprehensive, integrated approach to energy-sector cybersecurity is critical across physical infrastructure, policy frameworks, and implementation. Based on wide experience, we present three urgent issues with associated suggested policy and implementation recommendations with potential benchmarks for milestones as-suggested in President Biden’s recent Executive Order on Cybersecurity.

**General Background:**

Many individual points of excellence exist within the Energy ecosystem. It is time to develop and implement widely cohesive cybersecurity policies that stretch from requirements-building, through procurement and implementation to audit. Cohesive policy is hampered by a lack of practitioner cybersecurity knowledge in contracting corpus at Energy (and related Agencies such as Department of Defense, Department of Transportation, and Department of Commerce). As recent, systemic cybersecurity events such as SolarWinds and Colonial Oil have demonstrated, nationally-scoped systems have developed chained and complex interdependencies. A singular, compliance-based approach to cybersecurity that begins at the jumping-off point (Energy transmission and distribution) is no longer sufficient to ensure systemic cybersecurity concerns and an ever-widening attack surface.

**Issues and Solution Opportunities:**

1. Risk Scoping.
	1. Currently, risk scoping for catastrophic, damaging, or recoverable threat is murky in cyber-physical systems due to industry’s emphasis on the “Availability” bar of the Confidentiality-Integrity-Availability (CIA) cybersecurity triad which in turn is based on need for operational uptime.
	2. Risk scoping mechanisms exist in cybersecurity frameworks, however, these can be emphasized or de-emphasized by managerial decisions about what is, and is not, in scope for evaluation. (In one instance, we learned of a BES that used NERC CIP pre-audit activities as a reason to completely suspend ordinary cybersecurity activities [such as patching and vulnerability scanning] due to resource constraints and the concomitant decision to name neglected subsystems as out of scope.)
	3. Additionally, corporate tendency has been to use Single Loss Occurrence (SLO) and Annualized Loss Expectancy (ALE) calculations to determine risk, thus enabling decisions to “accept” (defer) risk that should remain in scope due to its multiplexed nature with potentially catastrophic second- and third-order effects to American security, the American economy, and America’s position in the global economy. We need to do a better job of helping the C-suite understand the cost to mitigate cybersecurity threats, versus the total cost of compromise, which is a combined qualitative/quantitative calculation performed by cybersecurity professionals that treats Loss of Operational Revenue + Cost to Return Business Operations + Loss of Reputation + Regulatory Costs. To this, we suggest, BES should consider the threat of broad civil liabilities in the event of a major operational cybersecurity event that can be definitively traced to mis-applied risk acceptance.

*Recommendation 1: Establish mandatory risk scoping boundaries for BES down to 3rd tier suppliers in addition to the mechanical aspects of risk allocation established by cybersecurity frameworks. Prevent corporations from accepting risk on BES and operations infrastructure that are known to have chained dependencies.*

*Suggested Milestone: Pilot a public-private consortium exercise to re-scope shared risk, with reports to DoE and Congress on re-defining “acceptable risk” per Federal cybersecurity milestones, in 2023 DoE Federal Budget Request.*

1. Buy American.

As President Biden stated in his April address to Congress, “The blade to a wind turbine in Pittsburgh should not be manufactured in Beijing.”

* 1. We strongly recommend that Energy support buy-American provisions in Supply Chain Risk Management provisions (such as those proposed by the revised NIST 800-161 rr1). Below, b) discusses Buy American in a security services context, and c) discusses Buy American in a manufacturing context.
	2. Buy American should be deployed when engaging assessors for BES and supply chain to the lowest tier. To use a particularly troublesome example from a partner Agency, the Department of Defense currently allows non-US companies to become accredited auditors for DoD’s Cybersecurity Certification Maturity Model assessments on its entire supply chain. We acknowledge that even if the vendor has the supply chain risk mitigation basic requirements in place, if there is compromised sourced components this causes a problem.
	3. This could be an opportunity to partner with Allied countries to diversify our supply chain and move towards creating resilient systems where any single point of failure is reenforced with the resilience of having a different product being able to complete the same task. This would also eliminate two of the same products offering redundancy but susceptible to the same attack, as is currently prevalent in Industrial Control System manufacturing and its security surveillance products.

*Recommendation 2: Establish comprehensive Buy American policies that shoot through procurement for security services (software, consultant services); manufacturing partnerships; and software bills of manufacture (SBOM).*

*Suggested Milestone: By end of FY 2022, provide Lead Agency draft language for inclusion in FAR/DFAR and wide Agency adoption to require Buy American provisions. By end of FY 2023, pilot an exemplar procurement-mep-sbom cybersecurity integration cycle with a goal for FY2024 implementation.*

1. Incentives. Incentives should encompass education and training (para a), below) as well as dual-use technologies (para b), below) that enable people-hours for critical thinking and systems curation versus mere security responsiveness.
	1. The best investment in the BES is by incentivizing utilities to send people to further their skillsets and become as educated as possible on developing threats, best practice mitigation techniques and encouraging them to take an active role to think independently and creatively. If we can foster an environment of highly motivated, and enabled individuals, these individuals will be able to convey the story to the C suite effectively.
	2. Encourage business to invest in technologies that improve efficiencies, compliance objectives, *and* security objectives. It is difficult to do all three without a long term strategy in place. You can have the best technology in any given area of ICS/OT security, yet people are the most scarce resource and also most difficult cost to justify. Invest in technologies that integrate across platforms to reduce manual workload. Many great technologies never produce full ROI because people are too busy to use them to their full potential.
	3. Offer programs that reward ingenuity. Compliance-only cybersecurity has unfortunately become a place where organizations suffer from paralysis by analysis and checkbox minimalism. This is not an environment that rewards creative minds to implement mitigating controls without a lot of administrative overhead. The adversaries we are encountering adapt quickly. To meet them on equal footing, we need to be more flexible in our approach to encourage people to innovate and for quick Federal adoption. Our end game is the continued reliable operation of the Bulk Electric System. This is done most efficiently when people are free to share information and implement quickly. They need to be encouraged to share information and those mitigation techniques need to be able to be adopted quickly to meet the adversaries on equal footing.

*Recommendation 3: Energy should pilot, then adopt, strategic initiatives that have a 3 to 5 year window to enable the DoE and partner Agency ecosystem to plan and implement incentives that improve skillsets, dual-use technologies, and approaches that reward ingenuity. Suggested Milestone: In FY 2023 – 2030, obligate appropriations for undergraduate and graduate scholarships at public colleges and universities. In FY 2023-2030, obligate appropriations for developing integrated cybersecurity technologies via SBIR, Congressionally-directed pilot, and small business set-aside procurements. Additionally, obligate funds for open challenges similar to those funded by DARPA.*

**Professional Backgrounds of Submitting Parties:**

**PFES, part of** [**The Planet Group**](https://theplanetgroup.com/), provides consulting, advisory, risk, and compliance services to organizations in the energy, utility, heavy infrastructure and industrial markets. With a headquarters in Chicago and 16 locations worldwide, we’ve been delivering innovative consulting solutions since 2012. Being a part of the Planet Group puts PFES in a unique position to integrate global knowledge and provide clients with well qualified resources from a network of over 500,000 consultants.   PFES has executed over $30B in capital projects since our founding in 2012.  PFES has emerged as a leader in providing cybersecurity consulting services for Industrial Control System (ICS) and Operational Technology (OT) environments. Our cybersecurity consulting organization is composed of cybersecurity subject matter experts and former NERC CIP auditors with extensive ICS/OT credentials and experience implementing cost-effective, comprehensive solutions that will not impact operations.

**Dominick Birolin**, Vice President of Cyber Services | CISSP, CISA.

Dominick Birolin has 25 years’ experience in IT & ICS/OT, audit and compliance experience across a broad range of industries. Mr. Birolin has 11 years of NERC CIP experience in the Energy Industry. Most recently he served as Senior Cybersecurity Analyst for Archer International where he led NERC CIP compliance and served as the Subject Matter Expert (SME) on Industrial Control Systems (ICS) Environments and Regulatory Compliance. He has also held senior Cybersecurity roles with Wurldtech, a GE Company, and North American Energy Alliance LLC (Essential Power, LLC) as well as technology SME roles with AT&T Managed Internet Service. Mr. Birolin holds a bachelor’s degree in information technology from Phoenix University and completed the CIO Executive Counsel Pathways Leadership Program

**Ampere Industrial Security**, LLC

Ampere Industrial Security is an international cybersecurity solutions consultancy founded by Patrick C. Miller.

**Patrick C. Miller**

Patrick Miller has dedicated his career to the protection and defense of critical infrastructures. As President and CEO of Ampere Industrial Security, he is a trusted independent security and regulatory advisor for industrial control systems worldwide. In addition to his role at Ampere, Mr. Miller is also the founder, director and president emeritus of EnergySec and US. Coordinator for the Industrial Cybersecurity Center. Patrick's diverse background spans the Energy, Telecommunications, Water, Wastewater, Manufacturing and Financial Services verticals including key positions with regulatory agencies, private consulting firms, utility asset owners and commercial organizations. Patrick Miller currently holds or has held the following professional certifications: Certified Information Systems Auditor, Certified Risk and Information System Control, Certified Information System Security Professional, Information Systems Security Architecture Professional, Systems Security Certified Practitioner, National Security Agency Infosec Assessment Methodologies, Certified Ethical Hacker, and Chemical-Terrorism Vulnerability Information.

**FullCircle Communications, LLC**

FullCircle is a mature boutique cybersecurity consultancy in operation since 2006. FullCircle participates in Federal and State cybersecurity projects with an emphasis on policy development and implementation; audit and assessment; and education. FullCircle also serves the micro-small-business community.

**Larisa Breton**, President / Founder

Larisa Breton is a seasoned cybersecurity professional with a dual focus on cybersecurity practice and education/training. She was deputy program manager for the Congressionally-mandated, cross-component Platform Resilience Mission Assurance program at DoD, where she supported a major policy development portfolio for control systems cybersecurity at OSD with major throughputs to Energy via the DoD’s Office of Installations and Energy (OIE). Larisa is also a senior cybersecurity consultant to the California Manufacturing Technology Consortium, a NIST MEP partner. She is a subject-matter expert on cybersecurity in industrial supply chains and the NIST cybersecurity frameworks. Larisa also has pioneered cybersecurity curricula for several Universities, and is a Digital Fellow at the University of Alaska SE (Juneau). She currently serves on the NIST National Initiative for Cybersecurity Education (NICE) subcommittee for cybersecurity apprenticeships ROI; the GSA’s cross-agency committee on federal building cybersecurity commissioning; and the Industrial Control Systems Joint Working Group’s Security Requirements Guide subcommittee.

**Conclusion and Signed:**

Thank you for this opportunity to submit to Department of Energy’s Request for Information. If we may provide any additional information, working group participation, or public testimony we would be honored to be of service.

Respectfully Submitted,

Dominic Birolin Patrick C. Miller Larisa Breton

Vice President President President

PFES Ampere Industrial Security FullCircle Communications