



Secure the Grid Coalition

2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

Dear Secretary Granholm and distinguished members of the Secretary of Energy Advisory Board:

The *Secure the Grid Coalition* greatly appreciates the opportunity to voice recommendations to the SEAB for consideration during its January 25, 2022, virtual meeting.

Our Coalition respectfully recommends:

- (1) that the Department of Energy **test the multi-million-dollar transformer donated by Duke Energy** in South Carolina. The last Administration did not, despite numerous requests, and there is still no real-world data on the effects of EMP on a transformer under load (only modeling from industry-funded studies that dangerously underestimate the effects). See Enclosure (A). – which is our response to the most recent DOE RFI on the energy supply chain – for more details.
- (2) that the Department of Energy **establish a Security Technical Implementation Group (STIG)** to work with industry **to address two massive cyber vulnerabilities to the electric grid:**
 - a. **Cyber vulnerabilities associated with engineering/management of power flows** between eight separated Grid regions as explained by former NSA CIO George Cotter in Enclosure (A).
 - b. **Sensor vulnerabilities associated with process sensors**, which currently have no cyber security, authentication, or cyber logging as explained by Joe Weiss in Enclosure (B).
- (3) that the Department of Energy **adopt a new “Energy Earthshots” Initiative** that could be named the **“Carbon Free Millenia.”** This concept involves the use of all-hazards secure advanced nuclear reactors and spent nuclear fuel **to provide up to 1000 years of clean power** and is further explained in Enclosure (A). We recommend you **work with willing state governments, such as New Hampshire**, which established a commission to study nuclear power and nuclear reactor technology, in part to explore this concept, as can be seen in Enclosure (C).

Our Coalition is ready to assist the SEAB and can make personal introductions to numerous experts throughout the country who can help DOE act on the above recommendations. Please see the enclosures for more details.

Respectfully submitted by,

Thomas J. Waller Jr.
Co-Director
Secure-the-Grid Coalition
twaller@centerforsecuritypolicy.org

Douglas Ellsworth
Co-Director
Secure-the-Grid Coalition
doug.ellsworth@usapact.org

Enclosure (A) - STG-Coalition-Letter to DOE on Supply Chain RFI Jan 2022

Enclosure (B) - Joe Weiss Comments on DOE RFI 1-13-22

Enclosure (C) - NH Legislation Establishing Commission to Study Nuclear Power



Secure the Grid Coalition
A Project of the Center for Security Policy
2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

January 14, 2022

U.S. Department of Energy
1000 Independence Ave, SW
Washington, DC 20585

VIA www.regulations.gov/docket/DOE-HQ-2021-0020

Comments of Secure the Grid Coalition Regarding Request for Information (RFI) on Energy Sector Supply Chain Review, Docket Number DOE-HQ-2021-0020

Dear Department of Energy:

Our Secure the Grid Coalition¹ has long worked to improve the security of our nation's most critical infrastructure – the electric grid. We recognize that a prolonged and widespread electrical blackout would cripple every one of our nation's 16 critical infrastructures, causing immense harm to our economy, our people, our national security, and – especially – our environment.

We appreciate DOE providing the opportunity for public comment on the important topic of the Energy Sector Supply Chain. We recognize that your Request for Information (RFI) sought information on specific questions, many of which pertain to energy sector asset owners and/or vendors. While our Coalition is comprised of nationally renowned security professionals drawn from a wide range of experiences and expertise (some of which do own or operate energy sector assets), our comments will focus more from the “outside looking in” perspective. Because our Coalition and its members receive no funding from the energy industry we are an unconstrained, unbiased observer and we believe that our observations are important to share with civil servants in government who are working diligently to “keep the lights on” every day.

Our response contains some answers to specific questions posed in the RFI, a re-addressal of concerns we voiced to the previous administration that were never acted upon, and an exciting idea that we suggest could become a new “Energy Earthshots Initiative” of the Department of Energy to help achieve the Biden Administration's U.S. jobs, economic, and emissions goals. [This idea affects the RFI's Area 7: Nuclear Energy Technology as well as Area 14: Commercialization and Competitiveness with respect to new and innovative actions that can encourage commercialization of U.S. innovation and increase U.S. competitiveness.]

A New Energy Earthshots Initiative - a “Carbon-Free Millenia”

On March 31st President Biden delivered remarks from a union training center in Pittsburgh, Pennsylvania where he unveiled his infrastructure plan and discussed the importance of America leading the world in the area of clean energy. He said, “We have to move now. I'm convinced, if we act now, in 50 years, people are going to look back and say this was the moment that America won the future.” Then on April 26th, during the Leaders Summit on Climate on Earth Day, President Biden charged your agency with “speeding the development of critical technologies in a suite of innovation areas” – leading

¹ The Secure the Grid Coalition is an ad hoc group of policy, energy, and national security experts, legislators, and industry insiders who are dedicated to strengthening the resilience of America's electrical grid. It is parented by the Center for Security Policy, a 501(c)(3). More info can be found here: www.SecureTheGrid.com

to Secretary Granholm’s announcement about the promising “Energy Earthshots Initiative.” We believe there is an idea worth becoming an “Earthshot” that, if executed wisely and rapidly, could achieve President Biden’s “moment that America won the future.”

This new “Earthshot” idea is to create a “Carbon-Free Millenia” with a “new renewable” clean source of energy. This would be done by recycling the roughly 90,000 metric tons of existing spent nuclear fuel to power all-hazards resilient fast reactors which could provide clean energy for America for up to 250 years and the existing stockpiles of depleted uranium to provide power for another 750 years for a combined 1,000 years. These reactors could be similar to those developed at Argonne National Laboratory in the 1960s and can be designed to be resilient to even the most catastrophic threat to the electric grid – nuclear electromagnetic pulse (EMP)² – like the small modular reactor (SMR) now already under development by NuScale³.

Many experts have warned for years about the hazards of spent nuclear fuel. Most recently, the U.S. Air Force’s Electromagnetic Defense Task Force (EDTF) made “Nuclear Power Resilience” its top priority.⁴ The EDTF warned that if a solar storm or nuclear EMP attack caused a pro-longed and widespread blackout, nuclear plants and their spent fuel could become a major hazard. “In a worst-case scenario, all reactors within an affected region could be impacted simultaneously. In the United States, this would risk meltdowns at approximately 60 sites and 99 nuclear reactors, with more than 60,000 metric tons of spent nuclear fuel in storage pools.”

Genuine environmental stewardship would call for the recycling of this spent fuel rather than risking it causing a future environmental catastrophe. And the use of fast reactors and their fuel – spent nuclear waste and depleted uranium stockpiles – would reduce nuclear proliferation concerns as well, since it could reduce the long-term need for uranium enrichment, eliminate conventional nuclear reprocessing (which requires plutonium separation) and last up to 30 years versus the roughly 18-month fuel cycle for conventional light water reactors.

While the “Carbon-Free Millenia” may seem like a lofty idea, it can become a reality. There are already companies developing fast reactors with these capabilities. For example, General Atomics Electromagnetic Systems (GA-EMS) has developed the Energy Multiplier Module (EM2) - an advanced small modular reactor (SMR) that can run on spent nuclear fuel.⁵

Investments in the research and development needed to field all-hazards secure advanced fast reactors can be drawn from not only from President Biden’s “American Rescue Plan” and the recently signed \$1.2 trillion “Infrastructure Investment and Jobs Act,” but also the \$40 billion (including interest) of funds collected by Congress for the purpose of securing a used nuclear fuel long-term solution.

A leading proponent of this concept of a “Carbon-Free Millenia” is a veteran of DOE and a member of our Secure the Grid Coalition and the Readiness Resource Group: Steven Curtis. Mr. Curtis routinely points out the importance of the DOE working with state governments to make this possible and suggests that a state be selected to build a “Carbon-Free National Laboratory.” Such a laboratory could conduct the fuel recycling as well as research on next-generation nuclear reactors, fuel types, microgrid technology, military reactor applied research, and a prototype pyroprocessing/fast reactor systems.

² <https://www.forbes.com/sites/jamesconca/2019/01/03/can-nuclear-power-plants-resist-attacks-of-electromagnetic-pulse-emp/?sh=2797ac7f70cb>

³ <https://www.nuscalepower.com/benefits/built-for-resilience/protected-against-emp-threats>

⁴ https://media.defense.gov/2018/Nov/28/2002067172/-1/-/1/0/LP_0002_DEMAIO_ELECTROMAGNETIC_DEFENSE_TASK_FORCE.PDF

⁵ <https://www.ga.com/nuclear-fission/advanced-reactors>

At the below link is a white paper authored by Mr. Curtis titled “A Short Case for Recycling Used Nuclear Fuel” which will be a helpful resource to more fully appreciate the value of this concept of a “Carbon-Free Millenia.”

<https://virginia-recycles-snf.com/wp-content/uploads/2020/03/A-Short-Case-for-Recycling-Used-Nuclear.pdf>

At the below link is a short article by Rabbi Yechezkel Moskowitz, a policy consultant for American technological and industrial sovereignty. The article builds on the concept of a “Carbon-Free Millenia” by exploring the history of nuclear recycling, policy approaches in other nations that would benefit American energy needs, the implications of a U.S. nuclear recycling program, and its effects on national security.

<https://centerforsecuritypolicy.org/nuclear-power-has-a-nuclear-waste-problem-heres-how-to-fix-it/>

President Biden said his “American Jobs Plan is the largest increase in our Federal non-defense research and development spending on record.” We hope that this increase in spending can be used to conduct the type of research needed to achieve the “Carbon-Free Millenia” through the use of a “new renewable” clean energy: all-hazards secure advanced reactors using recycled spent nuclear fuel, providing base-load power for 1000 years. Our Secure the Grid Coalition is ready to help DOE explore this new “Earthshot” idea at your convenience.

[Answers to Specific RFI Questions](#)

[Topic Area 5: Electric Grid—Transformers and HVDC](#)

Question 6. What other input should the federal government be aware of to support a resilient supply chain of this technology?

Answer 1: Testing Duke Energy’s Large Power Transformer

We have notified DOE multiple times about the urgent need to test Large Power Transformers (LPTs) against realistic electromagnetic spectrum (EMS) and cyber threats and that there exists in South Carolina a multi-million dollar transformer that has been *donated* for that specific purpose. Pictured below is that LPT. It was donated by Duke Energy to the U.S. Government’s Savannah River National Laboratory (SRNL) and Clemson University to be tested against realistic electromagnetic spectrum (EMS) threats such as High Altitude Electromagnetic Pulse (HEMP) and Intentional Electromagnetic Interference (IEMI) as well as realistic cyber threats. This transformer has been sitting idle and deteriorating for over three years for lack of less than a million dollars from your Department of Energy (DOE) to ship it up the Savannah River to SRNL to prepare it for testing in an already prepared location. Our Coalition believes that this inaction is absolutely unacceptable, and that this transformer should be immediately transported and funded for intensive, but easily affordable, testing according to proposals submitted to the DOE many months ago. If DOE requires point-of contact information for those involved with donating this transformer as well as appropriate DOE points-of-contact, please contact us (our POC information at the bottom of this document.)



Answer 2: Disclosing the Results of Large Power Transformer Inspection by Sandia National Laboratories

During the summer of 2019, a 500,000lb electric power transformer of Chinese manufacture was seized by federal authorities at the Port of Houston and carted, at no small expense, to Sandia National Laboratories in Albuquerque, New Mexico for sophisticated examination. It is quite a drastic action to deprive a utility of a transformer of that size because the expecting utility would be back at the “far end of the line” again without the transformer that it expected immediately.

Prior to this Federal action, an in-service transformer of the same origin was discovered to have embedded circuitry that was beyond design specifications in Ault, Colorado. There has been no official disclosure about what was discovered in that transformer or in the one examined by Sandia.

Utility companies nationwide, as well as the public have read publicized accounts of the transformer seizure yet have received no official word of any findings. A former intelligence official at the National Security Council commented in an interview stating that, “They found hardware that was put into the Transformer that had the ability for somebody in China to switch it off.” Couple that comment with Secretary Granholm’s reply of “Yeah, they do,” when asked if foreign actors have the ability to make the power grid go dark and both the public and the utility industry are left wondering: How does one “switch-off” a power transformer?

Transformers are either energized or de-energized. Switching hardware that controls whether a transformer is energized or de-energized normally reside some distance from the transformer itself and are not integrated into the transformer unit itself. This raises a critical question: “What can be integrated into a large power transformer that can cause it to stop functioning?”

Without a disclosure of the Sandia findings, utility companies and the trusting public are left to their own imaginations to determine how their transformers could be vulnerable. As an example, consider the pump that circulates the coolant inside the transformer. This pump could be the very piece of hardware that could be switched off remotely by China. Continuing this speculation, at the same time pumps are disabled, sensors that measure temperature, current, and voltage, could be spoofed by the same implanted circuitry to convey that everything is functioning well – even when the transformer is overheating with nothing to prevent the complete destruction of the transformer itself. The transformer is now “switched-off.” To the non-technical person this would seem like quite a stretch of the imagination, but to a person with a technical background, this scenario is not at all improbable.

It would solve many of the supply chain issues regarding the maintaining of a reliable and secure electric power grid by disclosing the findings of the Sandia investigation. It is reasonable to assume that very few utilities would knowingly purchase an unsafe, unreliable, and insecure transformer that could be turned

off perhaps when it's needed the most. In the absence of disclosure to utilities, large scale purchases and importation of additional transformers of Chinese manufacture continued into 2022. Thus, we believe the time is now for sufficient disclosure to assure that electric utilities are adequately forewarned.

Answer 3: Rectifying Threat from Foreign Transformers to Critical National Security Infrastructures

Given the risks associated with foreign-made transformers, we recommend that for all transformers supporting national security infrastructure, defined as DOD, Defense Industrial Base, intelligence agencies, the FBI, and US water systems, etc.) DOE should mandate an “Inspection, Repair, Rip and Replace” Program, paid for with federal funds (not ratepayer dollars,) to determine whether extra, mislabeled or below par electronics are embedded in transformers already installed in the US grid.

For those transformers already on order to be imported to the US, DOE should mandate an inspection and certification program to assure compromising or mislabeled electronics are not installed. The Inspection, Repair, Rip and Replace program should also apply to incoming imported transformers.

Finally, we also hope that through this RFI, DOE will identify manufacturers of electric power transformers and similar equipment for grid (and others) that are located in the USA and publish this information to the electric utility industry.

Topic Area 13: Cybersecurity and Digital Components

Question 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?

We believe the federal government must immediately prioritize protection of the *existing* Bulk Power System from all hazards. Since this topic area and its associated questions focus predominantly on cybersecurity, we direct you to the research of George Cotter, one of the world’s most experienced cryptologists. Mr. Cotter began his service to our nation as an intelligence analyst in the U.S. Navy. He joined the National Security Agency in 1952 and served there for more than forty years, rising to the rank of the organization’s Chief Information Officer (CIO.)

Mr. Cotter has deeply studied gaps in the cybersecurity protection regime for the Bulk Power System. He submitted to the Federal Energy Regulatory Commission (FERC) five (5) “Motions to Intervene” (MTIs) on various dockets. His research required study of four industry compliance audits of either CIP Standards or a parallel massive, independent set of Engineering Standards.

The latter, in existence long before CIP, were essential to industry management of power flows between eight separated Grid regions. FERC and NERC Regulators structured CIP standards so they would not interfere with those “Operations”, directly violating the law (Federal Power Act as amended 2005) which legislated CIP Standards. **These five MTIs have not been responded to by FERC in any related 2020 orders and notices.**

We summarize each MTI below and provide a hyperlink to the actual document and include the following excerpts:

“The Bulk Power System is a cybersecurity nightmare, almost totally susceptible to Supply Chain attacks, when, as and if a nation/state adversary chooses. FERC, NERC and industry efforts have conspired to create a regime that almost totally isolated Operational activities from federal cybersecurity regulation; substituting an almost meaningless structure limited to individual facilities, ensuring the continued protection of utilities from federal security oversight.”

Mr. Cotter also provided the following “Exposure Summary”:

“[E]xperts in the five or six critical infrastructures, including...national security functions, have grave concerns and some actual experiences (i.e., malware-related election intrusions), in the capabilities of the Russian Federation to seriously disrupt the Grid. The current Congress in bi-partisan frustration created the Congressional Cyberspace Solarium Commission to address cyber threats to the nation and is strongly recommending a National Deterrence Policy. That key finding is driven by a prior Defense Science Board Deterrence recommendation directly coupled to national security risks of a Grid takedown. FERC has had this filer’s interventions on precisely this evolution, yet continues abetting these risks from the [Russian] Federation out of deference to other industry priorities.”

Mr. Cotter provided a succinct history of the evolution of Critical Infrastructure Protection (CIP) standards:

“Growth and Grid integration had succeeded well until the major Northeast power outage of 2003, a cascading outage that exposed deep technical and operational flaws in the Grid. The joint US/Canadian study that followed for almost two years resulted in a major rewrite of the Energy Power Act of 2005. Cybersecurity had emerged over the previous decade that raised national concerns on the vulnerability of critical infrastructures including the electric Grid, and Congress added a new section 215 to the EPA [and the Federal Power Act] that empowered an industry “not for profit” corporation, NERC, as the Electric Reliability Organization (ERO) responsible for developing cybersecurity standards for the Bulk Electric System and the Federal Regulatory Energy Commission for their oversight.”

Critical Infrastructure Protection (CIP) Standards

“The evolution of CIP Standards occurred out of the public and congressional consciousness but did extensively involve industry leadership, exercising control of the NERC Board of Trustees, a substantial NERC staff with oversight of a succession of standards bodies, and FERC which ultimately had to go through the formalities of public review of standards. Industry positions on contentious issues were strongly supported by active industry organizations, NEI, EPRI, etc. However, **cyber vulnerabilities were seldom discussed and threats, almost never. As the Russian Federation began incursions in 2012 (supply chain penetrations) and active attacks in 2014 (with extensive malware testing in the Ukraine in 2015 and 2016), NERC and FERC showed little inclination to link cyber standards to BES vulnerabilities and Federation threats.** An FBI report on the 2014 incursions was never publicly released.”

Mr. Cotter’s Five Motions to Intervene were submitted between April and November 2020. Their main thrust was to document inadequacy of cybersecurity protection for the Bulk Power System, the core of the power supplied to the State-regulated Distribution Systems.

Summaries are below:

1st MTI on Docket No. EL20-46-000

This Docket covered an associate's complaint focused on the lack of transparency in Regulatory actions on Critical Infrastructure Protection violations by utilities, and the conflict of FERC Order No. 850 with Executive Order 13920. The MTI added to the complaint Supply Chain vulnerabilities, and more importantly, documents the deliberate Commission policy of dissembling on security standards, the distortion and suppression of vulnerabilities in the North American Grid, and a conspiracy of cover-up actions in regulatory management of ERA Section 215 responsibilities to protect critical electric infrastructure. As one example of two totally independent Engineering and CIP standards, the MTI contains a table summarizing over 476 pages of critical "**operational**" protection systems standards, whose cyber assets are absolutely devoid of cybersecurity wrappings.

Link:

<https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-1stMotion-FERC-11Jun20.pdf>

2nd MTI on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000

This MTI focuses on a FERC Staff paper proposing increased Tariff incentives for utilities voluntary cybersecurity investments; an absurd initiative given documented avoidance of CIP Standards. The MTI challenges FERC to show what Operational facilities are covered by CIP Standards, to identify actual cybersecurity CIP linkages to the independent Engineering Standards, and identify CIP measures to protect **Synchrophasor** networks, (Map provided). FERC did not respond, simply because they couldn't address these documented shortcomings. The MTI contains documentary evidence of a Duke Energy CIP Compliance Audit which challenges FERC to show how 127 separate CIP violations could be found with complete absence of linkages to the non-CIP Engineering Standards involved.

Link:

<https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-2ndMotion-FERC-25Jun20.pdf>

3rd MTI on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000

Building on a recent joint Cybersecurity Advisory titled "**NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems**" that focused on OT and Control Systems known to be vulnerable to malware attacks, this joint guidance issuance had the BES OT and Control Systems directly in its gunsights. This MTI contains a succinct description of the conflict FERC found itself in at the inception of CIP Standards in dealing with eight separate Reliability Regions insisting on absolute protections for regional variances from CIP Standards interference. It summarizes the convolutions NERC went through to structure CIP Standards around the Engineering Standards. The MTI contains yet another detailed study of a non-CiP Engineering Standards audit that documented avoidance of Operations and Real Time Power Flows, two no-no's in industry efforts to maintain tight control from FERC on inter-regional Grid relationships.

Link:

<https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-3rdMotion-FERC-7Aug20.pdf>

4th MTI on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000

This MTI deals with a number of issues, some raised in previous MTIs. It does include a detailed examination of a non-CIP compliance audit of CAISO, one of the largest Independent Systems Organizations in the US, consisting of over one hundred separate utilities. The purpose of the audit is not revealed but is believed to have been necessary due to a shift in Regional Entity responsibility back from PEAK Reliability to the WECC. IT appears to have been “pro forma”, checking a box. But it does reveal what had been seen in previous assessments, little or no action on anything related to Operations or Real Time Power Flows. Also discussed is a decade-long debate between FERC and NERC over need for CIP Standards governing Control Center to Control Center communications; NERC was holding the bag on resisting, due to direct conflict with the identical issue embodied in non-CIP Engineering Standards, all in FERC Order no. 866.

Link:

<https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-4thMotion-FERC-14Sept20.pdf>

5th MTI on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000

This MTI reveals direct couplings between Transmission and Distribution systems in Interconnection Regions that are essential for Grid operations, modernization and reliability, but impossible to justify on CIP Standards grounds; i.e., the interconnection of “CIP-protected” BES facilities with non-CIP Distribution systems, notably **Synchrophasor** networks, without cybersecurity interface protections. **Synchrophasors** are a major engineering innovation that has completely muddled the CIP, non-CIP picture; consequently NERC and FERC religiously avoid their citation. Evidence from Dominion Energy, CAISO, So. California Edison, NEISO, Bonneville Power Association, and TVA of this conflict is presented. A “Forced Oscillation Event” is described that demonstrates the criticality of **Synchrophasors**.

Link:

<https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-5thMotion-FERC-18Nov20.pdf>

Question 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?

To answer this question, we would like to direct you to the recommendations of another member of our Secure the Grid Coalition, retired U.S. Army Command Sergeant Major Michael Mabee. **At the below link** is a letter he sent to the White House, addressed to Chris Inglis, Office of the National Cyber Director and also to the Secretary of Energy Advisory Board (SEAB) on October 28, 2021.

<https://michaelmabee.info/wp-content/uploads/2021/10/Letter-to-the-Office-of-the-National-Cyber-Director-2021-10-28-R.pdf>

This letter contained his recommendations on how to encourage the private sector to include national security risk considerations in their business risk decisions. Specifically, Mr. Mabee recommended that Congress “enact legislation mandating that reasonably prudent actions on cybersecurity, physical security, EMP/GMD protective measures and hardening for severe weather events be taken by all entities, public or private sector, that are part of the critical electric infrastructure” and that “these measures must be certified periodically by the Chief Executive Officer of each such critical electric infrastructure entity.”

He recommends further that the Chief Executive Officer of each critical electric infrastructure entity be required to certify periodically to the Department of Energy (DOE) and the Department of Homeland Security (DHS) that they have reasonably prudent security measures to address hazards from cyber threats, physical threats, electromagnetic threats, solar weather, and terrestrial weather.

We also recognize that, short of such legislated mandates and associated penalties, over time, the best incentives for the owners and operators to secure their infrastructures from threats and hazards are not likely to come from governments or regulators, but rather large investment capital firms and insurance companies, particularly if those firms cease to insure companies which do not meet cybersecurity standards and best practices.

For example, control systems cybersecurity expert, Joseph M. Weiss, explained⁶, “[B]ased on history, Moody’s (and other credit rating agencies) participation may be the only way to get senior management to take appropriate actions to address control system cyber security, and thus, reduce enterprise risk.”

Additionally, the Associated Press reported⁷ that AXA, one of Europe’s top five insurers, “will stop writing cyber-insurance policies in France that reimburse customers for extortion payments made to ransomware criminals.”

We suggest DOE work with credit rating agencies and insurers to educate them on the important role they can play in this area. Involving these entities and having them refuse capital and/or insurance to insecure infrastructure owners who neglect security sends a strong message to both the private industry defenders and the criminal attackers. Industry cannot count on being “bailed out” and thus must assign a higher priority to cybersecurity, while criminals must change their own calculus by understanding there will be a reduced likelihood that their attacks will be successful.

Re-Addressed Concerns

Nearly two years ago, under the previous administration, DOE requested information on the supply chain for the bulk power system [FR Doc. 2020–14668] and our Coalition submitted comments and recommendations. As best we can tell, none of these comments or recommendations have been acted upon.

We would like to re-address those concerns, which included the need to (1) remedy direct current (DC) and EMP vulnerabilities to Large Power Transformers, to (2) prohibit the use of foreign sourced robotics (such as drones) which highlight grid vulnerabilities, to (3) withstand foreign and domestic lobbying for

⁶ <https://www.controlglobal.com/blogs/unfettered/finally-a-key-to-the-boardroom-for-control-system-cyber-security-moodys-steps-up/>

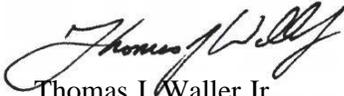
⁷ <https://apnews.com/article/europe-france-technology-business-caabb132033ef2aeee9f58902f3e8fba>

“business as usual” approaches to grid security, and to (4) demand that personnel and organizations trusted with U.S. Government collaboration cut ties with foreign adversaries.

Our 2020 letter can be found at this link: <https://securethegrid.com/wp-content/uploads/2021/02/STG-Coalition-Comments-on-DOE-RFI-24-Aug-2020.pdf>

In conclusion, our Secure the Grid Coalition would like to offer you and your staff any and all assistance we can provide to help you rapidly implement the recommendations we have made. We hope that these comments will provide you with helpful suggestions and that you will take action upon them posthaste.

Sincerely,

A handwritten signature in blue ink, appearing to read "Thomas J. Waller Jr.", written in a cursive style.

Thomas J. Waller Jr.

Director, Secure the Grid Coalition

Contact: info@SecureTheGrid.com

RFI: Supply Chain Review

Individual responder and industry expert–
Joseph Weiss, Applied Control Solutions
10029 Oakleaf Place Cupertino, CA 95014
(408) 253-7934
Joe.weiss@realtimeacs.com

Notice of Request for Information (RFI) on Energy Sector Supply Chain Review

I am submitting comments on DOE's Notice of Request for Information (RFI) on Energy Sector Supply Chain Review. My comments do not fall neatly into the categories identified in the RFI which I believe is part of DOE's problem in securing the grid.

The energy sector industrial base is exactly that – an industrial base. The process sensors, actuators, drives, invertors, circuit breakers, transformers, etc. are used in EVERY industrial base. Additionally, the cyber vulnerabilities in those analog and digital devices are common to every commercial and industrial sector. Those devices have no cyber security, authentication, or cyber logging. The push for renewables will make process sensors even more important as the control strategies for dispatching renewables is much more complex than the control strategies for dispatching “central station” power and will require a very significant increase the number of process sensors. Renewable resources are good for the environment and reduce consumer costs, but they are not a panacea to reducing electric grid cyber threats as utility-scale solar facilities can utilize hundreds of thousands to millions of solar panels with little to no cyber security creating a larger cyber threat surface than in a conventional fossil power plant.
<https://www.controlglobal.com/blogs/unfettered/renewable-resources-can-increase-cyber-threats/>

December 29, 2021, Ankit Suthar published the article “Are your smart instruments secured?”
<https://www.linkedin.com/pulse/your-smart-instruments-secured-ankit-suthar/?trackingId=7r%2Bf25P7QXKo83zDDsPZkw%3D%3D>. The article states: “We have been doing the commissioning of more than 3000 smart instruments I started to dig into all the manuals and datasheets of **different vendors** and found out that **there is no password at all in most of the instruments, even by default. You simply plug in your HART communicator and change whatever you want.**”

Consider how this design vulnerability defeats a zero-trust model. There is also an additional message that passwords may not be relevant for many process sensors and other control system field devices

Process sensors are ubiquitous and are under the auspices of the engineering organizations. Process sensors are the input to control and safety systems and provide input for operator decisions. Like our fingers, eyes, and ears that provide input to the brain to make the right decisions, if the process sensor input is not secure and accurate, catastrophic failures can occur. This has often meant that attention to safety, which the engineering organizations understand, has outrun attention to security, which is something that the engineering organizations have tended to view as the responsibility of the IT organization. And in turn, the IT organizations have tended to overlook process sensor security, seeing that as an engineering responsibility that's outside their own scope. At the process sensor level, however, safety and security are really the same issue.

The RFI requests identifying areas where collaboration between the government and private sector, as well as between government entities, is necessary to expand the energy industrial base, **what private sector leadership might look like in this area**, and where or how government can help.

I have a concrete suggestion that will help all operational sectors. In fact, we actually turned this into action by holding a meeting January 5th, 2022 with standards development and industry organizations to address the lack of cyber security in process sensors. The details follow:

[Interested industry representatives meet to discuss process sensor security and safety](#)

On December 14, 2021, I gave a Tech Talk to the IEEE Consultant Network Seattle Affinity Group of Seattle Section. As a result of that presentation, IEEE's Sheree Wen expressed an interest in identifying and addressing standards organizations' gaps and vulnerabilities associated with the cyber security and resiliency of control system field devices, including process sensors. Consequently, a virtual meeting was held January 5th, 2022 under the purview of IEEE, with universities and standards development and industry organizations representing a cross section of critical infrastructures. Essentially, "a coalition of the willing". As the process sensors are used in all sectors, the intent of the meeting was to create outcomes and a way forward for advancing cyber security and reducing risk associated with insecure process sensors in a common manner.

The Challenge of securing process sensors

Some example process sensor cyber-related incidents include:

- Dam collapse from erroneous low-level readings
- Sensor malfunctioned resulting in the release of 10 million gallons of untreated wastewater
- Safety relief valve in a nuclear plant did not lift because the pressure sensor never reached its setpoint (now consider the Triton cyberattack)
- ONE voltage sensor failure in combined cycle plant in Florida caused a 200MW load swing at the plant that resulted in a 50MW load swing in New England
- Tank farm explosions from erroneous level sensing
- Airplane crashes from erroneous sensor readings
- Refinery explosion from erroneous sensor readings

As the building industry was not present, there was a linked-in note on January 5, 2021, that the first ever cybersecurity standards specifically for building control systems was issued built on the widely accepted ISA/IEC62443 series of standards. September 2021, the Oak Ridge National Laboratory (ORNL), Pacific Northwest National Laboratory (PNNL), and National Renewable Energy Laboratory (NREL) issued the report Sensor impacts on building and HVAC controls: A critical review for building energy performance. According to the report, "Cybersecurity threats are increasing, and sensor data delivery could be hacked as a result. How hacked sensor data affects building control performance must be understood. A typical situation could include sensor data being modified by hackers and sent to the control loops, resulting in extreme control actions. To the best of the authors' knowledge, **no such study has examined this challenge.**"

Process sensors have no cyber security, authentication, or cyber logging. Consequently, it is not possible to know whether these incidents were intentional or malicious but made to look like they were unintentional.

There are three questions that are often asked about cyber security of process sensors:

- Do you need a physical presence to compromise the sensor? No, it can be done remotely.
- How much harm can cyber-related sensor impacts cause? The field calibrator calibrates one sensor at a time but connects insecurely to the Internet each time. The Asset Management Systems (AMS) has access to possibly tens of thousands of sensors. Meanwhile, the AMS has insecure connections to the Internet and often is connected to the Corporate Enterprise Resource Planning (ERP) systems. Also, see the real cases identified above.
- What happens when the compromised sensor data is sent to the cloud to be used in big data analytics for IOT or Industry4.0 applications? The sensor data being sent to the cloud is assumed to be secure.

These deficiencies lead to a need for a training environment to:

- Better understanding of how an adversary may interrupt, degrade, or possibly damage and destroy infrastructure.
- Develop forensic capability to detect process sensor cyber-related issues.

It should be noted that an appropriate training facility would be able to accomplish the above tasks for any condition, whether malicious or unintentional.

Process sensor security may amount to a gap in standards and regulation

Three discoveries and events the week prior to the meeting elevated the groups concerns.

- Based on discussions with the Transportation Security Administration (TSA), the recognition that the TSA pipeline cyber security guidelines did not address control systems including the sensors.
- The “discovery” in Abu Dhabi that more than 3000 sensors had no ability to have passwords <https://www.controlglobal.com/blogs/unfettered/a-vulnerability-worse-than-log4j-and-it-can-blow-up-facilities-and-shut-down-the-grid/>.
- The recent API 1164 pipeline cyber security guidelines (August 2021) effectively excluded the process sensors (Clause 6.6.5.4 (b) "Inventory should **not** include individual instruments that are not network connected").

As the cyber insecure sensors in the Abu Dhabi petrochemical plant show, digital sensors have built-in backdoors for performing remote calibration and other maintenance activities. That makes sense as a convenient, labor-saving design feature. It makes the sensors easier to upgrade and maintain. These same backdoors, however, can be exploited as vulnerabilities, even when the sensors do not appear to be connected to networks (see the problem with the API standards). In essence, the backdoor in the process sensors allows for two-way communication to/from the Internet with no cyber security protection. An indication of the disconnect between engineering and cyber security is that many engineers would be willing to pay extra to have the backdoors because it makes their jobs easier despite the cyber risk. The same cyber vulnerabilities in the process sensors also exist for the field calibrators and the AMS. At the 2016 ICS Cyber Security Conference, both the U.S. Air Force Institute of Technology (AFIT) and the Russians demonstrated how process sensor cyber vulnerabilities could be exploited. The Russian demonstration exploited the cyber vulnerability in the AMS while the AFIT presentation addressed the cyber vulnerability of multiple process sensors.

Organizations attending

The January 5th discussions were held under Chatham House rules so there were no names or attribution. The meeting included representatives from numerous industry, non-profit, and academic institutions:

American Gas Association (AGA)
 American Society of Mechanical Engineers (ASME)
 American Petroleum Institute (API)
 American Water Works Association (AWWA)
 FieldComm Group
 International ElectroTechnical Commission (IEC)
 Institute Electrical and Electronic Engineers (IEEE) changed name to ‘Advancing Technology for Humanity’
 International Congress on Systems Engineering (INCOSE)
 International Society of Automation (ISA)
 Food and Agriculture (Infragard)
 American Bureau of Shipping (Maritime)
 Mining and Metals
 MITRE
 Pharmaceuticals
 National Fire Protection Association (NFPA)
 National Commission on Grid Resilience
 Society of Automotive Engineers (SAE)
 Utilities (electric, water, energy)
 University of Indiana
 University of Texas-San Antonio
 Washington University

Progress, but much work remains

The participants recognized that considerable progress has been made for control system (Operational Technology-OT) network security. For example, guidance now exists with the ISA/IEC-62433 standards,

NIST SP800 series standards, and various other guidance documents. However, these standards do not yet address cybersecurity considerations at the lower levels of the Purdue Reference Model, namely Levels 0,1 (process sensors/devices) and field sensor networks. The group concluded that additional research, training, and testing to improve process sensor cyber security is lacking and requires new and innovative efforts from both industry and government leaders.

The discussions must be trans-disciplinary and must include engineers and facility operators as well as IT and OT networking personnel. The numerous actual control system cyber incidents clearly demonstrate that current approaches fail to sufficiently consider the engineer/operator roles and responsibilities in identifying and mitigating threats. There is consensus that engineers' contributions to security and resilience will be stifled if the perception continues to be viewed that control system cyber security is just network and IT/OT problems. One of the attendees noted "this is less about cross-industry than it is about cross-discipline. Limitations in one discipline (e.g., instrumentation-sensors) can lead to vulnerabilities in another like security." Consequently, this is not industry or sector specific. It requires the cooperation between physical security, network security, and engineering/operational security disciplines which can be fostered and enhanced via collaboration between professional associations and societies like IEEE, ISA, ASME, etc. To summarize, the networking community currently dominates cyber security and views all sectors as effectively being an extension of IT (<https://www.controlglobal.com/blogs/unfettered/ot-network-security-often-does-not-view-control-system-devices-and-the-process-as-their-problem>). Meanwhile, the engineering community has limited participation in cyber security decision making process as the engineering equipment that is often vulnerable is ignored by networking cyber security (<https://www.controlglobal.com/blogs/unfettered/engineering-operations-and-maintenance-often-do-not-view-cyber-security-as-their-problem>). A cross-disciplinary approach represents an important first step in bringing the engineering discipline to help address the cyber security of control systems which is generally not done when the focus is just securing the networks. To demonstrate the feasibility of a cross-discipline approach, a mining project in Canada was discussed that was using raw process sensor monitoring for productivity and maintenance improvements. As cyber security was also involved, the project brought multiple organizations together - corporate, plant engineering, operations, maintenance, safety, and cyber security. This project demonstrates that a cross-discipline approach is possible (in fact, necessary).

The group identified there are two distinct categories of process sensors to be addressed:

- Legacy devices - These are the devices currently in use and those still being built. There is no cyber security in these devices or cyber security standards to address these device limitations.
- Nextgen devices - Nextgen is still "on the drawing board" .ISA/IEC62443-4-2 can address these devices. However, at today's funding level, Nextgen is arguably 5 years from a prototype.

Historically, the network community has questioned whether process sensors should be within the scope of cyber security efforts. They question if process sensors are computers and if they are on networks. Process sensors may not look like computers, but they have similar components such as microprocessors which perform familiar computing functions. Sensors are also on networks, often serial as opposed to routable networks. The confusion may arise because many in the networking community view networks as being routable networks and therefore don't recognize serial networks as being networks. This can be seen in the NERC CIP standards which only recognize routable networks.

A way forward for process sensor security

The group concluded that establishing standards and guidelines to address the unique gaps and vulnerabilities with legacy field devices remains a priority. Despite the value of tools such as the MITRE ATT&CK tool and the CVE methodology, more work is needed. The MITRE ATT&CK tool doesn't address process sensors and other control system field devices. This needs to be added based on actual cases. The CVE methodology for software vulnerabilities has no counterpart for control system hardware. This also needs to be added.

Participants felt that consideration should be given to establish a Sensor STIG (Security Technical Implementation Group). There should be some sort of threaded discussion board where discussions could continue after this meeting. There was also the question as to what organizations are best suited to

sponsor and oversee this new and expanding area of training and research for control system field device cyber security.

The team agreed to develop a White Paper to be shared with government policy makers and R&D organizations who are able to resource and facilitate these efforts. The white paper will clearly define what is unique about legacy control system field devices and what needs to be done to provide improved cyber security as funding is necessary to expedite developing cyber security standards, frameworks, recommended practices, and information sharing for this inter-sector community.

Historically, standards have been driven by industry. It's time for the industry that relies on process sensors to take the lead in closing the gap between cyber security and safety engineering.

Respectfully,
Joe Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC

HB 543 - AS INTRODUCED

2021 SESSION

21-0728

06/11

HOUSE BILL **543**

AN ACT establishing a commission to study nuclear power and nuclear reactor technology in New Hampshire.

SPONSORS: Rep. Ammon, Hills. 40; Rep. J. Osborne, Rock. 4; Rep. Vose, Rock. 9

COMMITTEE: Science, Technology and Energy

ANALYSIS

This bill establishes a commission to investigate the implementation of nuclear reactor technology in New Hampshire.

Explanation: Matter added to current law appears in ***bold italics***.
Matter removed from current law appears ~~[in brackets and struckthrough.]~~
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

HB 543 - AS INTRODUCED
- Page 2 -

1 (i) One member of the public, appointed by the governor.

2 II. Legislative members of the commission shall receive mileage at the
3 legislative rate when attending to the duties of the commission.

4 III. The commission shall investigate:

5 (a) Advances in nuclear power technology, including “generation IV” reactors, by
6 conducting research and seeking counsel and testimony from experts in the field;

7 (b) The most promising generation IV designs as determined by the Gen IV
8 International Forum:

9 (1) Gas-cooled Fast Reactor (GFR);

10 (2) Lead-cooled Fast Reactor (LFR);

11 (3) Molten Salt Reactor (MSR);

12 (4) Supercritical Water-cooled Reactor (SCWR);

13 (5) Sodium-cooled Fast Reactor (SFR); and

14 (6) Very High Temperature Reactor (VHTR);

15 (c) Large-scale, small-scale, microreactor, modular and breeder reactor designs;

16 (d) The safety of modern designs, including “passive safety systems”;

17 (e) Various types of fuel consumption, including the ability for new designs to safely
18 consume nuclear waste, such as the waste in long-term storage facilities;

19 (f) Nonelectric applications including:

20 (1) Hydrogen or other liquid and gaseous fuel or chemical production;

21 (2) Water desalination and wastewater treatment;

22 (3) Heat for industrial processes;

23 (4) District heating;

24 (5) Energy storage; and

25 (6) Industrial or medical isotope production;

26 (g) Potential siting options;

27 (h) Partnerships with industry participants or investors;

28 (i) Partnerships with federal agencies, such as the U.S. Nuclear Regulatory Commission;

29 (j) Federal incentives for nuclear power generation; and

30 (k) Shall identify potential obstacles with federal nuclear regulation.

31 IV. The members of the commission shall elect a chairperson, vice chairperson, and clerk
32 from among the members. The first meeting of the commission shall be called by the first-named
33 house member. The first meeting of the commission shall be held within 60 days of the effective
34 date of this section. Six members of the commission shall constitute a quorum.

35 V. The commission shall submit interim reports of its findings and any recommendations for
36 proposed legislation to the speaker of the house of representatives, the president of the senate, the

HB 543 - AS INTRODUCED

- Page 3 -

1 house clerk, the senate clerk, the governor, and the state library on or before December 1, 2022 and
2 July 1, 2023, and shall submit its final report on or before December 1, 2023.

3 3 Repeal, RSA 125-O:30, relative to a commission to investigate the implementation of nuclear
4 reactor technology in New Hampshire is repealed.

5 4 Effective Date.

6 I. Section 3 of this act shall take effect December 1, 2023.

7 II. The remainder of this act shall take effect upon its passage.