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

Follow Up Comments of David Jonas Bardin June 6, 2021

For: Michael Coe, **ElectricSystemEO@hq.doe.gov**

Dear Mr. Coe,

I submitted Preliminary Comments on April 23, 2021, in response to the RFI published at 86 Federal Register 21309 (Vol. 86, No. 76, April 22, 2021). Herewith my Follow Up Comments, as promised.

My perspectives

Vulnerabilities of our electric infrastructures, and weaknesses in previous Administration's attempted approach, concern me based on my experiences in and out of government:
— I served in the then-new DoE, under its first two Secretaries, as a Senate-confirmed Presidential appointee (having previously served as the Deputy Administrator of the Federal Energy Administration).
—Today, I am an 88-year-old retired member of Arent Fox, LLP, whose *pro bono* activities have included electric reliability and infrastructure issues.
—Earlier, I held civil service and SES positions at the Federal Power Commission (1958-69) as trial attorney, assistant general counsel for legislation and rulemaking, and deputy general counsel.

These Follow Up Comments, a day before RFI deadline, are my personal views, submitted solely on my own behalf. They ask DoE to consider some alternative hypotheses in light of References, below.

References .

[1] North American SynchroPhasor Initiative (NASPI), Webinar May 26, 2021, *Digital Voltage and Current Sensors* [https://naspi.org/sites/default/files/2021-05/20210526_naspi_webinar_nugrid.pdf]

[2] Rebecca Smith, *How America could go dark*, WSJ July 14, 2016
[3] Rebecca Smith, *U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny*, WSJ May 27, 2020

[4] Rebecca Smith, *Texas Power-Grid Operator Should Enhance Emergency Units, Former Regulators Say,* WSJ June 3, 2021

[5] G. N. Ericsson, KTH Royal Institute of Technology, *Cyber Security and Power System Communications — Essential Parts of a Smart Grid Infrastructure*, IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 3, JULY 2010 [https://www.researchgate.net/publication/224133056_Cyber_Security_and_Power_System_Communication-Essential_Parts_of_a_Smart_Grid_Infrastructure]

[6] Tom Alrich's blog, April 29, 2021, *Finally, some information on the forthcoming software EO* [http://tomalrichblog.blogspot.com/2021/04/]

[7] Joe Weiss, *Process sensor issues continue to be ignored and are placing the country at extreme risk*, June 1, 2021 [https://www.controlglobal.com/blogs/unfettered/process-sensor-issues-continue-to-be-ignored-and-are-placing-the-country-at-extreme-risk/]

[8] Joe Weiss, *TSA cyber security requirements are still not addressing control system-unique issues*, May 27, 2021 [https://www.controlglobal.com/blogs/unfettered/tsa-cyber-security-requirements-are-still-not-addressing-control-system-unique-issues/]

[9] Comments of Mr. George R. Cotter, February 15, 2021, in FERC Docket No. RM21-3-000 [https://elibrary.ferc.gov/eLibrary/filelist?document_id=14929007&optimized=false]

Risks versus vulnerabilities; gaps in "critical infrastructure" to be protected

Although DoE asserts "the immediate imperative" to secure our "electric infrastructure," saying that the "electric power system is vital to the Nation's energy security, supporting national defense, emergency services, critical infrastructure, and the economy" and that: "Preventing exploitation and attacks by foreign threats to the U.S. supply chain is the focus of this Request for Information (RFI)," — asserting opportunities to "increase awareness" and "protections against high-risk electric equipment transactions", [1] the RFI does **not** increase awareness of risks and it fails to confront gaps in critical infrastructures which DoE does not even seek to protect.

For example, DoE creates a gap by excluding all operating systems such as synchrophasors instead of identifying at least many of them as critical infrastructures. See https://www.naspi.org/node/897 and Reference [1]. (Synchrophasors can provide real-time information about currents, voltages, frequency, and phase angles at nodes and hubs of the bulk electric power system (BES) as well as distribution systems which the BES serves.)

See, also, References [5], [6], [7], [8].

Synchrophasors are similarly excluded from critical infrastructure protection (CIP) standards set by the National Electric Reliabity Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). For a frustrated appraisal consider Reference [9].

My May 25, 2021, memorandum for Secretary of Energy (SoE) [reproduced in Appendix, below]

I understand that a Team is preparing and will send to SoE (some time after the RFI's June, 7, 2021, deadline) responses to my memorandum. DoE should weigh whatever responses that Team prepares, together with the RFI responses DoE receives before its RFI deadline expires.

Large transformer made in China now energized and operating at Ault CO substation near Denver

The substation at Ault CO is an asset of the Western Area Power Administration (WAPA), a component of DoE. WAPA goes through DoE on procurements which involve public solicitations. In 2014, DoE first opened a public solicitation ("DE-SOL") on WAPA's behalf for a large electric power transformer to be installed at Ault together with related parts and services. (See DE-SOL-0011343 for public record of this procurement, including amendments.)
— As amended 28 July 2017, WAPA sought bids including delivery, installation, testing, and energizing a large transformer. See Attachment A, Revised AMD 002, Ault KU1A Transformer Specifications.
—Also see Attachment E, Ault KU1A Transformer Questions and Answers, 28 July 2017.
I have asked WAPA to report when this transformer was energized (guessing that was before Reference [3] events).

---

[1] "On January 20, 2021, Executive Order, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,* suspended Executive Order, *Securing the United States Bulk-Power System,* for 90 days and directed the Secretary of Energy and the Director of the Office of Management and Budget (OMB) to consider whether to recommend that a replacement order be issued. In the process of developing such recommendations, [DoE] ... identified opportunities to institutionalize change, increase awareness, and strengthen protections against high-risk electric equipment transactions by foreign adversaries, while providing additional certainty to the utility industry and the public. As the United States Government considers whether to recommend a replacement Executive Order that appropriately balances national security, economic, and administrability considerations, [DoE] is seeking information from electric utilities, academia, research laboratories, government agencies, and other stakeholders on various aspects of the electric infrastructure."

Large imported transformer made in China, seized in Houston and trucked to Sandia National Laboratories (SNL) in 2019 for analysis (see Reference [3])

WSJ article (Reference [3]) reported seizure which happened in June 2019. DoE and Department of Homeland Security (DHS) may have instigated that seizure.
— Whoever instigated that extraordinary seizure must have been influenced by assessments of risk and concerns.about.vulnerabilites.
— If SNL analyses clearly confirmed reasons for seizure (or, contrariwise, clearly established that no good reasons existed after all), wouldn't DoE be wise to acknowledge as much in general terms?
— In either case (or any intermediate case), have experts at SNL (and possibly other National Labs) been asked to develop risk and vulnerabilities assessment tools and mitigation measures? If no, Why not? If yes, have results been responsibly disseminated?

Other large transformers imported from China

Hundreds of other large transformers have been imported from China (not to mention medium and small size transformers and other kinds of electric power system equipment). Will DoE need to learn where they are (at least in the BES)? When will DoE need to know?

Events at WAPA's Liberty substation near Phoenix AZ in 2016 (see Reference [2])

This WSJ reporting appears to reveal both lax attitudes to physical security and limited usefulness of closed circuit television (CCTV) as a practical deterrent to physical penetrations. In that case, CCTV showed that two people had penetrated, wandering inside the fence without challenge, but video was too fuzzy to identify either one.
— Has CCTV been more successful in other cases?
— If so, has DoE shared those facts effectively?

E-ISAC (Electricity Information Sharing and Analysis Center) issues

If E-ISAC learns of serious threats and vulnerabilities which involve classified information, can they share enough information to arm "frontline" 24/7 staff at exposed electric utilities who probably do not themselves have clearances? I have put this question to E-ISAC (by phone call) and ask DoE to do that, too.

Black start issues (see Reference [4])

Extreme cold weather events this winter revealed failure to weatherize generation units (including black start units), despite similar experience 10 years ago and FERC-NERC recommendations then. Review and reconsideration of NERC's black start unit standards deserves priority attention.

Please let me know if you have any questions.

Respectfully submitted, David Jonas Bardin

Appendix to RFI submittal: My May 25, 2021, memorandum for Secretary of Energy (SoE) Granholm

May 25, 2021

The Honorable Jennifer Mulhern Granholm, Secretary of Energy (SOE)
the.Secretary@hq.doe.gov

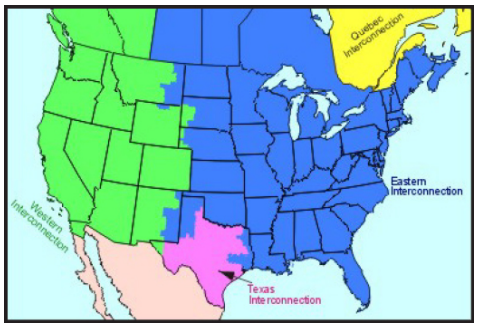
cc:
Acting Assistant Secretary (CESER) Puesh M. Kumar
Acting Assistant Secretary (OE) Patricia A. Hoffman

Re:
Is inadequate security at WAPA substations a threat to electric power grid?

From:
David Jonas Bardin, who served as Senate-confirmed appointee under the first two SOEs, now writing as a concerned private citizen

Dear Secretary Granholm,

The Western Area Power Administration (WAPA), which reports to you as a component of the Department of Energy (DoE), operates ten percent of the electric power transmission lines in the Western Interconnection. (Green area in National Academies Press map, below.)



In 2016, the Wall Street Journal (WSJ) highlighted inadequate WAPA security, especially at its Liberty substation near Phoenix, AZ, where repeated intrusions in 2013 and 2014 did serious damage. (See Rebecca Smith, Grid Attack: How America Could Go Dark, July 14, 2016, https://www.wsj.com/articles/how-america-could-go-dark-1468423254 and excerpts appended below.). WAPA's former Administratior told WSJ we have "taken steps to improve our physical security program and processes." (But his staff told WSJ that security budgets were barely 3% of needs). — Four years later, as shown (I am told) in 2020 photo below, WAPA did not even lock an unguarded gate into its Ault, CO substation and transformer yard which serve WAPA's 245 kV line between Wyoming's Powder River Basin and Denver, CO (an intertie between the Western and Eastern Interconnections).

— Is that gate at least padlocked today?

When WAPA seeks to acquire transformers (or other costly equipment), or to remove old transformers, DoE issues an invitation for bids (IFB) with an identifier#); its solicitation file — "DE-SOL" with an identifier # — may be amended from time to time. Moreover, the Buy American Act of 1933 applies to WAPA and governs large procurements — unless waived.
— For example, IFB No. 89503118BWA000003, was issued April 5, 2018, for the construction and completion of a 345-kilovolt (kV) capacitor bank at the Liberty Substation located in AZ for WAPA's Desert Southwest Region under a Small Business Set Aside.
— For another example, Federal Contract Opportunity for y--AULT SUBSTATION - STAGE 08 89503218BWA000007. - Power and Communication Line and Related Structures Construction - was posted Jun 20, 2018 by the Headquarters (DOE). Due Aug 14, 2018 (later accelerated). Work to include (among other things): "Remove and replace three (3) 167 MVA 345/230-kV power transformers designated KU1A-1, KU1A-2, and KU1A-3" and lay "foundations, conduit, conductors and cables for delivery of new three-phase 600 MVA transformer designated KU1A (GFE)."

Did WAPA acquire a new, large transformer, designed and manufactured in China, for its Ault substation? Is it designated KU1A? What were IFB No. and DE-SOL # for that procurement? Who waived Buy American Act for that procurement and when? When was that transformer delivered to Ault? When was it installed and placed in service? Do photos below portray it?

On May 27, 2020, WSJ reported that federal agents had seized a large, Chinese-designed and manufactured electric power transformer in the summer of 2029 at the Port of Houston, TX, and shipped it by truck to Sandia National Laboratories (SNL), one of DoE's "Crown Jewels" for analysis. See https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710?st=xeoz7t5bmbfbtd0&reflink=share_mobilewebshare .) WSJ reported that WAPA had imported that transformer.
— Have SNL's findings, conclusions, and risk mitigation recommendations been shared with WAPA?
— Has DoE seen to it that at least Senators Manchin, Barrasso, and Murkowski are fully briefed on SNL's findings and conclusions?

— If WAPA indeed ordered that seized transformer, what were to be the transformer specs, place of installation, and date of installation per the IFB and DE-SOL?
By choosing to clarify matters raised above, you may (a) reduce poisonous suspicions fueled by policies of excessive secretiveness set during the previous Administration, (b) enhance Executive - Congressional collaboration, and (c) protect the public you aim to serve.

Respectfully submitted, David Jonas Bardin

Appendix: Excerpts from WSJ July 14, 2016 (Reference [2]):

Utilities don't always report attacks despite a legal requirement to notify the Energy Department within six hours of any event that could interrupt electricity or if a break-in targets security systems.

No utility has been fined for failing to comply as far as he knew, said David Ortiz, deputy assistant secretary at the Energy Department: "I don't have an enforcement team."

The Journal found nine substation break-ins over the past two years where theft wasn't the apparent motive. The tally and details of the break-ins were gleaned from interviews and public records requests. The count included attacks affecting the federally owned Liberty substation in Buckeye, Ariz.

The substation, about 35 miles west of Phoenix, is a critical link in the southwest power corridor, delivering electricity to heat homes in northwestern states during winter and cool buildings in the southwest during summer.

On Nov. 5, 2013, someone slashed fiber-optic cables that serve Liberty, as well as the larger Mead substation near Hoover Dam. It took workers about two hours to re-establish proper communications and normal controls.

Liberty is operated by [WAPA], which controls 17,000 miles of high-voltage power lines used by utilities serving 40 million people in 15 states. If this system suffered a catastrophic failure, it would take down other utilities with it, experts said.

Alarms signaling trouble at Liberty began ringing at a utility operations center in Phoenix 13 days after the communications outage. Dozens of alarms sounded over two days before an electrician was dispatched.

The electrician expected a false alarm. Instead, he found the perimeter fence sliced open and the steel door to the control building "peeled back like a sardine can," said Keith Cloud, the utility's head of security.

The substation's computer cabinets were pried open. The substation's security cameras proved useless: eight of 10 were broken or pointed at the sky, Mr. Cloud said. Most had been out of operation for a year or more.

Two months later, on Jan. 30, 2014, Liberty was hit again. Two men with a satchel cut the gate lock and headed to the control building. They left after trying, unsuccessfully, to cut power to a security trailer outfitted with cameras and blinking lights, which were installed after the first break-in.

This time, Mr. Cloud said, utility officials found 16 of 18 security cameras had failed. Most were installed after the first break-in and hadn't been properly programmed. Investigators retrieved a single fuzzy video from a thermal-imaging camera.

Mark Gabriel, WAPA's administrator, said the utility has "taken steps to improve our physical security program and processes," including creating the security department in 2013 that Mr. Cloud now heads.

A federal audit faulted WAPA in April for violations of security regulations, including broken or obsolete equipment, lax control over keys to critical substations and failure to install intrusion-detection systems.

Mr. Gabriel said WAPA spends a couple of hundred million dollars on capital improvements annually, which includes money for security improvements. "The bigger story is how that break-in and others in the industry changed the thinking," he said.

Mr. Cloud said he has received about $300,000 for security upgrades at a handful of WAPA's 328 substations, including Liberty. To protect the system's 40 most important substations and control centers, he said, he needs $90 million: "I don't have the authority or budget to protect my substations."