From:	David Bardin
To:	SEAB
Subject:	[EXTERNAL] Remarks and attachments of David Jonas Bardin (pronounced BardDEEN) for SEAB, June 13, 2022
Date:	Monday, June 13, 2022 2:15:33 PM

Chris,
Please share the following with SEAB members. Thank you.
Faithfully, David

REMARKS OF DAVID JONAS BARDIN FOR SEAB, June 13, 2022 (and attachment thereto).

I bring 5 matters to your attention:

A)

Joe Weiss recently discovered evidence that a few times in 2018 and 2019, electric utilities in different States lost monitoring and control of their SCADA systems at *precisely* the same times and for *precisely* the same durations.

This was not due to weather nor telecommunication provider issues. The only logical explanation seems to be that **sophisticated attackers compromised control center SCADA for more than 30 minutes**.

[See "Utility/DOE data indicates sophisticated hackers have compromised US electric control centers - Submitted by Joe Weiss on Sun, 06/12/2022 - 17:37"

https://www.controlglobal.com/blogs/unfettered/utilitydoe-data-indicates-sophisticated-hackers-have-compromised-us-electric-control-centers] [See, also, Attachment A]

This new evidence deserves the SEAB's urgent attention and advice to Secretary Granholm as to its implications.

B)

Earlier, Joe Weiss published evidence that electric utilities, the National Electric Reliability Corporation (NERC) - and, perhaps, the Federal Energy Regulatory Commission (FERC) - suffer from self-delusion which leads them to deny existence, extent and scope of control system cyber incidents.

[See "https://www.controlglobal.com/blogs/unfettered/utility-industry-continues-to-deny-that-control-system-cyber-incidents-are-occurring/"]

These problems continue to deserve SEAB attention and advice.

C)

Dr. Jeffrey Love (who directs the USGS Geomagnetism Program) and six co-authors published an important article which, I understand, is being covered by Tommy Waller on behalf of the Secure the Grid Coalition. [See "Mapping a Magnetic Superstorm: March 1989 Geoelectric Hazards and Impacts on United States Power Systems." Available at the weblink:

https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1029/2021SW003030]

It merits intensive SEAB attention and advice to Secretary Granholm.

D) A NewScientist article suggests that some "stealth" coronal mass ejections (CME) are both speedier and more forceful than we have assumed and could give us far less time to prepare than we count on. NOAA's space weather experts are aware of stealth CMEs, but uncertain whether their scale might significantly impact operations and infrastructure on which we depend. Issues raised need to be explored, not allowed to fall between the cracks.

E) Dr. M. Gene Lim has expressed concern "that North Korea or China can turn **Nuclear Power Plants** into **Super Improvised Explosive Devices** (**IED**s) at their whim."

He is also concerned

> that, the Nuclear Regulatory Commission (like the Atomic Energy Commission before it) exacerbates vulnerability to blackouts and exposes strategic regions to chaos, destruction of infrastructure and loss of precious lives, by insisting that **S**imultaneous **L**oss of both **O**ffsite and **O**nsite **P**ower (**S-LOOP**) supply to nuclear power plants are [so] **"INCREDIBLE"** that they need not be planned against.

He believes that the facts are otherwise and writes as an 88-years-old, naturalized Korean-American 'hands-on' nuclear power engineer, with a Sc.D. in Applied Nuclear Science and practical experiences as a Westinghouse employee in Japan, South Korea, Spain, China.

I shall separately provide a set of slides, some of them revised slides, to illustrate Dr. Lim's concerns. He is probably the best informed expert in the USA on these issues, bringing to bear richly diverse perspectives.

I urge the SEAB to give Dr. Lim's concerns and analyses deep attention and to give their careful advice to Secretary Granholm.

Faithfully, David J. Bardin

Attachment [A] Joe Weiss wrote:

DOE's Form OE-417 collects information from the US utilities on electric incidents and emergencies. The OE-417 data covers the time span from 2000 through the end of February 2022 and so does not include any incidents since the start of the 2022 Russia-Ukraine War. There have been 37 cyberattacks identified, four of those cyberattacks lasted at least one and a half days with one lasting more than 4 months. There have been 150 "complete loss of view or control for more than 30 minutes" incidents reported since June 2018. several of these incidents lasted from 4 to 25 hours. Moreover, at least 11 of these incidents led to demand losses of at least 80 MW and, in one case, led to 130,000 customers losing power. There were several incidents where utilities in multiple locations had "loss of monitoring or control" starting at exactly the same time and ending at exactly the same time. Given it wasn't weather or a common telecommunication provider issue, the only logical explanation is that a

sophisticated attacker got simultaneous access to multiple utilities' bulk control center SCADA systems and shut off monitoring (and possibly took control). It is not a stretch to say that our adversaries could be practicing for more impactful attacks at a time of their choosing.

https://www.controlglobal.com/blogs/unfettered/utilitydoe-data-indicates-sophisticated-hackers-have-compromised-us-electric-control-centers

David Jonas Bardin
davidbardin@aol.com
djonasbardin@gmail.com
[redacted]