Thank you for the opportunity to address the SEAB. Given the reminder that Dr. Witherell gave at the beginning of the meeting that the national labs were created to solve the nation's big technical problems – I want to reiterate a big technical problem that DOE labs can and must address that I brought up at the last SEAB meeting.

Control systems consist of field devices such as process sensors and OT networks. The cyber security emphasis has been on computer networks, patching software, zero trust, and multi-factor authentication. Meanwhile, process sensors have no cyber security but are 100% trusted by the control systems and the operator and alarm displays that use the process sensor input. The sensors are insecure because the microprocessors have to be low enough power to not be subject to explosions from fugitive emissions.

It's instructive to emphasize the seriousness and immediacy of the threats and risks by providing a timeline of actual incidents illustrating that all the DOE jurisdictional infrastructures, facilities, and demonstration projects are cyber vulnerable, because all need to measure process conditions such as pressure, temperature, voltage, current, etc. using insecure process sensors. There have been many cases where process sensor cyber-related incidents have led to catastrophic failures and deaths.

1989 Identified Rosemount pressure transmitter oil-loss. This was a manufacturing flaw, that is a hardware supply chain issue. Safety-related pressure sensors with this flaw contributed to the TMI core melt.

2009 Stuxnet – the US attack was a compromise of 100% trusted sensor serial data to damage centrifuges (NERC CIPs exclude sensors and serial communications)

2015 AFIT dissertation on hacking multiple vendors' wired process sensors

2016 Russian presentation on hacking process sensors. AFIT presentation on hacking wireless process sensors and actuators

2017 Iran aware of my Defcon presentation on lack of cyber security in process sensors

2019 A failure of ONE process sensor rippled through the entire Eastern Interconnect causing a significant load swing more than a thousand miles away. The Chinese provided counterfeit pressure sensors to the North American market.

2021 ORNL, PNNL, and NREL performed a study of "Sensor impacts on building and HVAC controls: A critical review for building energy performance". The report noted that sensor data delivery could be hacked as a result resulting in potentially dangerous control loop swings. Yet, according to the Lab's, no such study has examined this challenge. ISA identified newest sensors fail 69 of 130 individual cyber security requirements (Safety sensors in an LNG facility was the use case); Abu Dhabi identified more than 3,000 smart instruments in a petrochemical facility with no passwords, even by default. You simply plug in your HART communicator and change whatever you want. These changes can blow up refineries, burst pipelines, release toxic chemicals, take over electric transformers, etc. with no cyber forensics

2022 January 5 Standards meeting with IEEE, ISA, ASME, SAE, AWWA, API, AGA, etc as there are no cyber security standards for legacy process sensors; March 10 Air Force Cyber College presentation – "Shields Up and Good Cyber Hygiene do not apply to insecure process sensors"; March 16 NIST manufacturing report acknowledges no security in modern sensors and actuators.

Process sensor calibration and maintenance tools have no cyber security and are directly connected to the web.

It is high irony – which puts our nation at grave risk – that our government facilities and energy infrastructures put "zero trust" in IT networks but put "100% trust" in their insecure sensors.

I ask the SEAB to *task your labs to help solve this problem* and stand ready to help them do it.

Thank you for your time and interest.

Joe Weiss