Appendix A – Irreparable Issues with S. 3688

Below are the reasons we our Secure the Grid Coalition believes that S.3688 exacerbates grid vulnerabilities and violates the public trust:

- **It appears to conflict directly with and counteract progress made by the Congressional Solarium Commission (CSC).** We have found that the bill could be a serious complication to the authorities, responsibilities and actions detailed in dozens of CSC-recommended organizational and legislative changes aimed at a more "federal" national cybersecurity program.

- **It codifies a major departure from the original intent for transparency & public disclosure.** The initial agreements established between the Federal Government and the electric power industry at the inception of the FERC/NERC regulatory regime were that this self-regulated industry was supposed to maintain a "high level of transparency and public disclosure" and ensure that members of the public would have access to and be able to participate in the rulemaking and enforcement regime. This bill shutters access to the public by:
    - Exporting the "Security through Obscurity" regime to other government agencies by offering assistance to those agencies in labeling information as Critical Energy Infrastructure Information (CEII) in order to prevent FOIA access;
    - Codifying government inaction and regulatory malfeasance by releasing FERC from any responsibility for untimely processing of FOIA requests, establishing that FERC's failure to grant or deny a request after (1) year from submission will automatically designate the requested information as CEII and for a period of 10 years.
    - Allowing blanket CEII designations for a duration that can be extended at the will of FERC (i.e., forever);
    - Allows utilities the freedom *not* to designate information as CEII until after it becomes the subject of a FOIA request;
    - Allows FERC to later designate information as CEII that they previously determined wasn't;
    - Establishes that FERC may grant CEII to a member of the public only if that member has entered into an NDA with the source of the information which has been approved by an administrative law judge from DOE or FERC.

  Again, it should be noted that this bill was filed following FERC's "White Paper" on transparency and Docket Docket AD19-18-000. On that docket, Former Chief Information Officer of the U.S. National Security Agency (NSA), George Cotter stated the following:

  > *"There are no security benefits that will accrue to the BPS by further denial of access to violations of CIP Standards. NERC E-ISAC is aware of this entire threat evolution. NERC should be held criminally liable should these capabilities ever be used against this nation. Instead, NERC jointly sponsors this industry biased White Paper thinly disguised as protective of the BPS, in reality intended to further insulate utilities from liability lawsuits, state PUCs, CIP compliance actions, and, of course, other Federal examination."*[1]

  Considering this, if S. 3688 were to become law and when a safety, reliability, or security violation causes a major blackout and loss of life and property, how will policymakers or the public ever ascertain who should be held liable? This is an unprecedented insulation from

[1] https://securethegrid.com/wp-content/uploads/2019/09/2019-09-12-Comments-of-George-Cotter-001433795044-1.pdf

liability for the federal regulators and the industry upon which every other industry depends and it comes at great expense to the public trust.

- **It establishes a parallel classification system not in the public interest & violates Executive Order 13526 of December 29, 2009 "Classified National Security Information"[2]:** The bill codifies "CEII" which has informally been established by the electric power industry and FERC as a parallel classification system that is not in the public interest and is in conflict with established federal guidelines. For example,
    - Section 1.2 of Executive Order 13562 states that *"Information may be classified at one of the following three levels: (1) Top Secret, (2) Secret, (3) Confidential*" and that *"Except as otherwise provided by statute, no other terms shall be used to identify United States classified information."*
    - *"Sec. 1.7. Classification Prohibitions and Limitations. (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:*
        (1) conceal violations of law, inefficiency, or administrative error;
        (2) prevent embarrassment to a person, organization, or agency;
        (3) restrain competition; or
        (4) prevent or delay the release of information that does not require protection in the interest of the national security."

As we have made clear in Appendices B through D, we have observed that since 2010, electric utilities have routinely used CEII as an excuse to conceal violations of law, inefficiency, and administrative error and to prevent embarrassment. This legislation gives those utilities free reign to expand this repugnant practice and maintain it indefinitely, to the great detriment of the public. It also prevents a concerned public from utilizing the Freedom of Information Act (FOIA) to ascertain which utilities have violated standards, broken laws, or put their ratepayers at risk.

- **It forces states to adopt inadequate cybersecurity standards, conceals risks to their ratepayers, and diminishes the emerging capabilities of the National Guard and Reserves to cyber defend critical assets in their states.** The bill forces the states to conform to the CIP standards which our Secure the Grid Coalition has pointed out are inadequate and rarely enforced. The bill also prevents state Public Service Commissioners from learning about risks to their rate payers. Finally, at a time when the SecDef, Service Secretaries, and the National Guard Bureau are exploring methods to identify and train National Guard and structured Military Reserve elements at each such state level for potential development for cybersecurity roles for the grid (and other) critical infrastructure defense, this bill constructs massive bureaucratic and administrative obstacles to that progress. The bill could force states that have already set up cyber units, and gained appropriate authorities therein, to go back to the drawing board with regard to information sharing.

- **It may violate the jurisdiction of other federal organizations and ruin their efforts at gaining public trust.** Attorneys in each of the affected federal agencies will have to take a close look at the bill, but on its surface it appears to violate the established jurisdictions of these agencies. For example, the Nuclear Regulatory Commission has worked diligently to involve the public on issues of safety and this bill could stifle those efforts and compromise the trust and confidence gained by the American public in the safety and security of the nuclear power industry if they thought that NRC could use the legislation to begin concealing information from public scrutiny under the guise of CEII.

[2] https://www.govinfo.gov/content/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf

- **Stifles needed changes in corporate culture which put the public at great risk.** This bill incentivizes utilities to continue obscuring from public and regulator scrutiny any and every vulnerability and/or issue of non-compliance with established safety, security, and reliability standards. The bill enables utilities to make up arguments on the fly that information is "CEII" in an effort to keep it from public view.

  Pacific Gas and Electric (PG&E) is a case study of how corporate culture that is lackadaisical about security and compliance puts its ratepayers at risk. This bill would further enable the types of egregious behavior that has already resulted in felony convictions, massive economic damages, and significant loss of life, on the part of PG&E such as:

  - Physical Security risks – a year after the now famous April 16, 2013 attack on PG&E's Metcalf substation, the same substation was breached in August 2014[3] and the utility's director of corporate security said publicly that PG&E has 'high level security' at critical facilities" while reporting internally that "In reality PG&E is years away from a healthy and robust physical security posture."[4] Further obscurity of physical security violations will only reinforce this type of dishonesty.
  - Safety risks – On July 31, 2009, PG&E was fined $100,000 for violating the transmission vegetation management standard. Then, after the NERC/FERC coverup began in 2010 there are violations this standard in the Western Interconnection. This is the same location where more than 86 deaths occurred in the "Camp Fire" – the deadliest and most destructive wildfire in California history. It is possible PG&E is a culprit but their identify remains concealed from public scrutiny.[5]
  - Cybersecurity risks – On May 30, 2016 cybersecurity expert Chris Vickery reported a massive data breach by PG&E. On February 28, 2018 NERC issued a "Notice of Penalty regarding Unidentified Registered Entity" in which the NERC-anonymized entity apparently agreed to pay penalties of $2,700,000 for very serious cybersecurity violations.[6] The PG&E data breach in 2016 and NERC's cover-up of the identity of the "Unidentified Registered Entity" — who by NERC's own admission was involved in a dangerous data breach — is ample proof that a watchful regulator is necessary to protect the bulk power system. Yet, it seems that regulator currently conspires with its Congressional overseers to further insulate the industry and itself from public scrutiny.
  - Economic risks – PG&E ultimately went bankrupt and now either the rate payer or the taxpayer will foot the bill for their recovery. In either case, how is it in the public interest that a utility be allowed to incur so many risks and yet be insulated so well from public scrutiny?

- **Stifles security and resilience investments & cost recovery mechanisms**: We observe that the Federal Power Act of 2005, section 215, was an unfunded mandate whereby utilities have been told they have to improve cybersecurity but that the cost recovery would come from Public Utility Commissioners. Utilities now face issues with paying for necessary security and reliability upgrades because they are a "victim of their own success" in obscuring from public scrutiny the challenges they face on these fronts since their violations have been covered up for so long. This bill will "codify that coverup" and enable even more safety, security, and reliability violations to be lumped in as "CEII" and further distance the industry from achieving cost recovery mechanisms. The bill severely disadvantages state public service commissioners in being able to maintain visibility over the industry's vulnerabilities, making the industry less capable of justifying rate increases to pay for resilience.

---

[3] https://www.mercurynews.com/2014/08/28/puc-launches-probe-into-breach-at-pge-substation-in-san-jose/
[4] https://michaelmabee.info/metcalf-attack-pge-security-memo/
[5] https://michaelmabee.info/transmission-vegetation-management/
[6] https://michaelmabee.info/grid-cybersecurity-comments-ferc/