September 14, 2022

Honorable Gary C. Peters
724 Senate Hart Office Building
Washington, D.C. 20510

Honorable Rob Portman
448 Senate Russell Office Building
Washington, D.C. 20510

Chairman Peters and Ranking Member Portman:

The undersigned trade associations, which represent almost all aspects of the U.S energy sector and its critical operations that serve customers reliably across North America and the world, appreciate the opportunity to share our comments regarding amendment #554, Section 5207 "Systemically Important Entities" (SIE), within HR 7900, the House-passed FY23 National Defense Authorization Act (NDAA).

Our members have worked diligently, in a strong collaborative partnership with Congress and the Administration, to develop and implement effective cybersecurity programs that help to prevent and mitigate attacks and vulnerabilities. We are working closely with our federal partners to inform reasonable incident reporting regulations as required in the recently passed Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) incident reporting regime contained in the FY22 Omnibus, HR 3600. We have also been diligently working towards compliance with the TSA pipeline security directives and are engaged in the development of reasonable pipeline cybersecurity regulations.

Our associations believe that the SIE proposal, as written, is not appropriate for inclusion in the FY23 NDAA. The program would provide the Department of Homeland Security (DHS) through the Cybersecurity and Infrastructure Security Agency (CISA) with the authority to designate individual critical infrastructure businesses and compel their participation in the SIE's reporting requirements without a clear understanding of the benefits and burdens of this program, which was detailed in recommendation 5.1 of the Cyberspace Solarium Commission (CSC) report on codifying "systemically important critical infrastructure." Further, the SIE proposal does not distinguish itself from existing programs, including: 1) the work of National Risk Management Center (NRMC) in identifying critical interdependencies, 2) reporting on software and technology supply chain dependencies as required by the Cybersecurity Maturity Model Certification (CMMC) for Department of Defense and other government contractors, and 3) prioritizing access to government services for entities deemed in the interest of national security, such as those represented by our associations. We strongly believe this proposal should move through the regular order process in Congress, where exposure to scrutiny would produce legislative improvements, and remove redundancies and duplication of authority in the SIE program.

It is also important to note that the SIE proposal comes on the heels of other enactments whose implementation is relevant to the authorities under development within the SIE program. These efforts – such as the CIRCIA reporting regulations and the requirements within the two SDs, as well as the forthcoming pipeline cybersecurity regulations that will ultimately replace the SDs – should be complete

in order to appropriately design the SIE authorities around those existing requirements. Our industry is actively engaged with TSA and CISA on these programs and participates in numerous voluntary cybersecurity initiatives. To authorize the development of a program that is already redundant to many of these efforts would be an ineffective use of industry and government resources during a time when cybersecurity expertise is already very thin.

We remain committed to our Cyber Security collaborative partnership and urge you to decline to include the SIE proposal in the FY23 NDAA.

American Fuel & Petrochemical Manufacturers
American Gas Association
Liquid Energy Pipeline Association
American Petroleum Institute
American Public Gas Association
Interstate Natural Gas Association of America