Policy Resolution 2.2019

Synchronizing Congressional Oversight and Legislative Measures on Cybersecurity

Originating Sponsor
Representative Jim Gooch, Jr., Kentucky

Co-Sponsor
Representative William E. “Bill” Sandifer, III, South Carolina

WHEREAS, the Twenty-First Century has brought forth a new age of innovation, automation, big data, artificial intelligence, blockchain technology, and machine learning, and America needs to be able to detect, respond, and prevent ever increasing cyberattacks, a growing and critical international warfare that is capable of serious impact on the functioning of government and industry; and

WHEREAS, the nation’s electric energy grid system, our energy resource supply and delivery infrastructure, finance, communications, election methodology, manufacturing, chemical industries, commercial process, defense industry and operations, emergency management, agricultural resources, government facilities and services, public healthcare, information technology, transportation, and water and wastewater systems are vital and critical to preserve the quality of life in America; and

WHEREAS, a dynamic threat environment exists across the nation due to the interconnection and interconnectedness of our data systems to other less critical infrastructure systems requiring strategic information sharing between government at all levels and the public and private sectors; and

WHEREAS, state governments are responsible for securing public networks, state digital infrastructure, and citizen data, and they must coordinate cybersecurity efforts with federal agencies and potentially affected public and private sector organizations; and

WHEREAS, in May of 2018, the Office of Management and Budget and the Department of Homeland Security determined that 71 of 96 federal agencies are at risk or high risk of cyber intrusions and are not equipped to determine how threat actors seek to gain access to information; and

WHEREAS, the public and private sectors are dedicating increased resources to education, training, and recruitment of cyber workers so that America is better protected from this insidious threat matrix.

THEREFORE BE IT RESOLVED, the Southern States Energy Board, meeting in Louisville, Kentucky, on September 24, 2019, urges the Congress to improve the synchronization of congressional oversight and legislative measures on cybersecurity. Congress must continue to clarify the roles and responsibilities of federal agencies in preparing for, responding to, and preventing cyberattacks; and

BE IT FURTHER RESOLVED, centralized authority, points of contact, and formalized communications are necessary to address increasingly complex threats. Congress must be aware that the
increasing number and inconsistency of federal security regulations is an unnecessary burden for state
governments and is an inefficient use of constrained security resources; and

**BE IT FURTHER RESOLVED**, the Southern States Energy Board recommends the restoration of the
position of White House cybersecurity coordinator to synchronize and harmonize disparate federal
regulations, coupled with a working group of key state and federal officials, to provide greater insight and
education on the complexity of the threat network of nefarious nation-states and methods used to repel
attacks; and

**BE IT FURTHER RESOLVED**, the Southern States Energy Board urges the federal government to
continue providing essential cybersecurity risk briefings and resources to our member states. We also
support the Department of Homeland Security’s Office of Cybersecurity and Communications for its
continued interaction with state chief information officials; and

**BE IT FURTHER RESOLVED**, the Southern States Energy Board urges the Administration to propose,
and Congress to provide, long-term authorization and appropriations for cybersecurity education and
workforce development to sustain the nation’s cybersecurity workforce.

*Unanimously adopted on September 24, 2019, at the*
*59th Annual Meeting of the Southern States Energy Board in Louisville, Kentucky*