



U.S. CHAMBER OF COMMERCE

October 20, 2020

The Honorable Marco Rubio  
Chairman  
Select Committee on Intelligence  
U.S. Senate  
Washington, DC 20510

The Honorable Adam Schiff  
Chairman  
Permanent Select Committee on Intelligence  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Mark Warner  
Ranking Member  
Select Committee on Intelligence  
U.S. Senate  
Washington, DC 20510

The Honorable Devin Nunes  
Ranking Member  
Permanent Select Committee on Intelligence  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Rubio, Chairman Schiff, Ranking Member Warner, and Ranking Member Nunes:

We write to encourage Congress to pass the Cyberspace Solarium Commission's (Commission) recommendations to improve intelligence information sharing between the government and critical infrastructure this year. Currently included in the Intelligence Authorization Act (IAA) passed by the House Permanent Select Committee on Intelligence (HPSCI) as provisions 605 and 606, we encourage Congress to retain the core goals of these provisions in conference. Congressional action is urgently needed to close this gap in cybersecurity policy and ensure the intelligence community and privately-owned critical infrastructure can collaborate effectively to protect against national security threats.

Critical infrastructure – such as those in the financial services, energy, and communications sectors – is under constant threat from nation-state actors and international criminal organizations seeking to disrupt or destroy systems on which the entire United States relies. Improving and standardizing collaborative efforts between the public and private sectors to better inform foreign intelligence collection, analysis, and strategic warning of attacks will help protect such infrastructure as national security assets.

Existing information sharing programs with the private sector are focused on broad information sharing, downgrading of intelligence about general threats, and victim notification. These laudable efforts have improved greatly in recent years with benefits across multiple critical infrastructure sectors. What is missing from these efforts is explicit recognition and codification of the need to use, and resource the use of, national intelligence capabilities to protect designated critical infrastructure as strategic assets. The Department of Homeland Security and Sector Specific Agencies play important roles and are critical partners with designated critical infrastructure; however, they cannot provide the foreign intelligence collection capabilities and analytic capacity of the intelligence community led by the Director of National Intelligence.

Nascent collaborative efforts between the federal government and the financial services, communications, and energy sectors exist. Thus, some may argue there is no need for the proposals we advance. In fact, it is in support of these efforts that we ask you to enact provisions 605 and 606 of the HPSCI IAA. There is no mandate that protects

these critical relationships. The codification of these important collaborative efforts would cement this relationship, enhance public-private coordination, and strengthen the overall economic and national security of the nation.

Just as the 9/11 Commission highlighted critical gaps in information sharing among government agencies that could have helped prevent the terrorist attacks of September 11, 2001, the Cyberspace Solarium Commission has flagged the need for greater sharing of intelligence with critical infrastructure that could help avoid a disastrous day for the nation. Critical infrastructure is already facing foreign attacks. We urge you to swiftly pass legislation to close this gap and improve our collective defense against foreign cyber threats.

Sincerely,

American Bankers Association  
Bank Policy Institute  
Edison Electric Institute  
U.S. Chamber of Commerce  
USTelecom