5.1.2 Codify Processes for Identifying Private Sector Cyber Intelligence Needs and Priorities

This proposal implements the Commission's recommendation to direct ODNI and DHS, in consultation with relevant sector-specific agencies, to conduct a six-month review on how to establish a formal process to solicit and compile private-sector input to inform national intelligence priorities, collection requirements, and more focused U.S. intelligence support to private-sector cybersecurity operations.

A BILL

To codify processes for identifying private sector cyber intelligence needs and priorities, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. STRENGTHENING PROCESSES FOR IDENTIFYING CRITICAL INFRASTRUCTURE CYBERSECURITY INTELLIGENCE NEEDS AND PRIORITIES.

(a) CRITICAL INFRASTRUCTURE CYBERSECURITY INTELLIGENCE NEEDS AND PRIORITIES.—

(1) IN GENERAL.—Not later than 180 days following the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and appropriate Sector-Specific Agencies, as defined by section 2201 of the Homeland Security Act of 2002, shall establish a formal process to solicit and compile critical infrastructure input to inform national intelligence collection and analysis priorities.

(2) RECURRENT INPUT.— Not later than 30 days following the establishment of the process required pursuant to paragraph (1), and biennially thereafter, the Director of National Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall solicit information from critical infrastructure utilizing the process established pursuant to paragraph (1).

(b) INTELLIGENCE NEEDS EVALUATION AND PLANNING.—Utilizing the information received through the process established pursuant to subsection (a), as well as existing intelligence information and processes, the Director of National Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(1) identify common technologies or interdependencies that are likely to be targeted by nation-state adversaries;

(2) identify intelligence gaps across critical infrastructure cybersecurity efforts;

(3) identify and execute methods of empowering sector-specific agencies to—

(A) identify specific critical lines of businesses, technologies, and processes within their respective sectors; and

(B) coordinate directly with the intelligence community to convey specific information relevant to the operation of each sector; and

(4) refocus information collection and analysis activities, as necessary to address identified gaps and mitigate threats to the cybersecurity of critical infrastructure of the United States.

(c) REPORT TO CONGRESS.—Not later than 90 days following the completion of the evaluation pursuant to subsection (b), and annually thereafter, the Director of National Intelligence and the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Homeland Security of the House of Representatives a report that—

(1) assesses how the information obtained from critical infrastructure is shaping intelligence collection activities;

(2) evaluates the success of the intelligence community in sharing relevant, actionable intelligence with critical infrastructure; and

(3) addresses any legislative or policy changes necessary to enable the intelligence community to increase sharing of actionable intelligence with critical infrastructure.

(d) DEFINITION OF CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).