# AMENDMENT TO THE RULES COMMITTEE PRINT OF H.R. 3523 OFFERED BY MS. JACKSON LEE OF TEXAS

At the end of the bill, add the following new section:

**SEC. 3. IDENTIFICATION OF CYBERSECURITY RISKS TO THE TRANSPORTATION SYSTEMS SECTOR.**

(a) IN GENERAL.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security, shall on a continual basis identify and evaluate cybersecurity risks to critical infrastructure to the transportation systems sector for inclusion in annual risk assessments required under the Department of Homeland Security National Infrastructure Protection Plan. In carrying out this subsection, the Secretary shall coordinate, as appropriate, with the following:

(1) The head of the sector specific agency with responsibility for critical infrastructure.

(2) The head of any agency with responsibilities for regulating the critical infrastructure.

(3) The owners and operators of critical infrastructure, including as a priority, the relevant Critical Infrastructure Partnership Advisory Council entities.

(4) Any private sector entity determined appropriate by the Director of National Intelligence and the Secretary of Homeland Security.

(b) EVALUATION OF RISKS.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the individuals and entities referred to in subsection (a), shall evaluate the cybersecurity risks identified under subsection (a) by taking into account each of the following:

(1) The actual or assessed threat, including a consideration of adversary capabilities and intent, preparedness, target attractiveness, and deterrence capabilities.

(2) The extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by a disruption, destruction, or unauthorized use of critical infrastructure.

(3) The threat to national security caused by the disruption, destruction or unauthorized use of critical infrastructure.

(4) The harm to the economy that would result from the disruption, destruction, or unauthorized use of critical infrastructure.

(5) Other risk-based security factors that the Director of National Intelligence, in consultation

with the Secretary of Homeland Security and, as appropriate, with the head of the sector specific agency with responsibility for critical infrastructure and the head of any Federal agency that is not a sector specific agency with responsibilities for regulating critical infrastructure, and in consultation with any private sector entity determined appropriate by the Director of National Intelligence, in consultation with the Secretary of Homeland Security, to protect public health and safety, critical infrastructure, or national and economic security.

(c) AVAILABILITY OF IDENTIFIED RISKS.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security, shall ensure that the risks identified and evaluated under this section are made available to the owners and operators of critical infrastructure within the transportation system sector.

(d) COLLECTION OF RISK-BASED PERFORMANCE STANDARDS.—

(1) REVIEW AND ESTABLISHMENT.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security, the National Institute of Standards and Technology, and the heads of other appropriate agencies, shall review existing internationally recognized consensus-developed risk-

based performance standards, including standards developed by the National Institute of Standards and Technology, for inclusion in a common collection. Such collection shall include, for each such risk-based performance standard, an analysis, based on the typical implementation of each performance standard, of each of the following:

(A) How well the performance standard addresses the identified risks.

(B) How cost-effective the standard implementation of the performance standard can be.

(2) USE OF COLLECTION.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the heads of other appropriate agencies, shall develop market-based incentives designed to encourage the use of the collection established under paragraph (1).

(e) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term ''critical infrastructure'' means any facility or function of a company or government agency that, by way of cyber vulnerability, the destruction or disruption of or unauthorized access to could result in—

(1) a significant loss of life;

(2) a major economic disruption, including—

(A) the immediate failure of, or loss of confidence in, a major financial market; or

(B) the sustained disruption of financial systems that would lead to long term catastrophic economic damage to the United States;

(3) mass evacuations of a major population center for an extended length of time; or

(4) severe degradation of national security or national security capabilities, including intelligence and defense functions, but excluding military facilities.

(f) LIMITATION OF REGULATORY AUTHORITY.—Nothing in this section expands the regulatory authority of sector specific agencies or other agencies with regulatory authority over elements of critical infrastructure beyond the risk-based performance standards collected under subsection (d).