AMENDMENT NO._____ Calendar No._____

Purpose: To require a comprehensive aviation cybersecurity framework and for other purposes.

IN THE SENATE OF THE UNITED STATES—114th Cong., 2d Sess.

S. 2658

To amend title 49, United States Code, to authorize appropriations for the Federal Aviation Administration for fiscal years 2016 through 2017, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. THUNE

Viz:

At the appropriate place in title II, insert the following:

SEC. _____. AVIATION CYBERSECURITY.

(a) COMPREHENSIVE AVIATION FRAMEWORK.—

(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration shall facilitate and support the development of a comprehensive framework of principles and policies to reduce cybersecurity risks to the national airspace

system, civil aviation, and agency information systems.

(2) SCOPE.—As part of the principles and policies under paragraph (1), the Administrator shall—

(A) clarify cybersecurity roles and responsibilities of offices and employees, including governance structures of any advisory committees addressing cybersecurity at the Federal Aviation Administration;

(B) recognize the interactions of different components of the national airspace system and the interdependent and interconnected nature of aircraft and air traffic systems;

(C) identify and implement objectives and actions to reduce cybersecurity risks to the air traffic control information systems, including actions to improve implementation of information security standards and best practices of the National Institute of Standards and Technology, and policies and guidance issued by the Office of Management and Budget for agency systems;

(D) support voluntary efforts by industry, RTCA, Inc., or standards-setting organizations to develop and identify consensus standards,

best practices, and guidance on aviation systems information security protection, consistent with the activities described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)); and

(E) establish guidelines for the voluntary sharing of information between and among aviation stakeholders pertaining to aviation-related cybersecurity incidents, threats, and vulnerabilities.

(3) LIMITATIONS.—In carrying out the activities under this section, the Administrator shall—

(A) coordinate with aviation stakeholders, including industry, airlines, manufacturers, airports, RTCA, Inc., and unions;

(B) consult with the Secretary of Defense, Secretary of Homeland Security, Director of National Institute of Standards and Technology, the heads of other relevant agencies, and international regulatory authorities; and

(C) evaluate on a periodic basis, but not less than once every 2 years, the effectiveness of the principles established under this subsection.

(b) THREAT MODEL.—The Secretary of Transportation, in coordination with the Administrator of the Federal Aviation Administration, shall implement the open recommendation issued in 2015 by the Government Accountability Office to assess the potential cost and timetable of developing and maintaining an agency-wide threat model to strengthen cybersecurity across the Federal Aviation Administration.

(c) SECURE ACCESS TO FACILITIES AND SYSTEMS.—

(1) IDENTITY MANAGEMENT REQUIREMENTS.—Not later than 1 year after the date of enactment of this Act, the Secretary of Transportation shall implement open recommendations issued in 2014 by the Inspector General of the Department of Transportation—

(A) to work with the Federal Aviation Administration to revise its plan to effectively transition remaining users to require personal identity verification, including create a plan of actions and milestones with a planned completion date to monitor and track progress; and

(B) to work with the Director of the Office of Security of the Department of Transportation to develop or revise plans to effectively transition remaining facilities to require per-

sonal identity verification cards at the Federal Aviation Administration.

(2) IDENTITY MANAGEMENT ASSESSMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Transportation shall prepare a plan to implement the use of identity management, including personal identity verification, at the Federal Aviation Administration, consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274; 15 U.S.C. 7464) and section 225 of title II of division N of the Cybersecurity Act of 2015 (Public Law 114–113; 129 Stat. 2242).

(B) CONTENTS.—The plan shall include—

(i) an assessment of the current implementation and use of identity management, including personal identity verification, at the Federal Aviation Administration for secure access to government facilities and information systems, including a breakdown of requirements for use and identification of which systems and facilities are enabled to use personal identity verification; and

(ii) the actions to be taken, including specified deadlines, by the Chief Information Officers of the Department of Transportation and the Federal Aviation Administration to increase the implementation and use of such measures, with the goal of 100 percent implementation across the agency.

(3) REPORT.—The Secretary shall submit the plan to the appropriate committees of Congress.

(4) CLASSIFIED INFORMATION.—The report submitted under paragraph (3) shall be in unclassified form, but may include a classified annex.

(d) AIRCRAFT SECURITY.—

(1) IN GENERAL.—The Aircraft Systems Information Security Protection Working Group shall periodically review rulemaking, policy, and guidance for certification of avionics software and hardware (including any system on board an aircraft) and continued airworthiness in order to reduce cybersecurity risks to aircraft systems.

(2) REQUIREMENTS.—In conducting the reviews, the working group—

(A) shall assess the cybersecurity risks to aircraft systems, including recognizing the

interactions of different components of the national airspace system and the interdependent and interconnected nature of aircraft and air traffic systems;

(B) shall assess the extent to which existing rulemaking, policy, and guidance to promote safety also promote aircraft systems information security protection; and

(C) based on the results of subparagraphs (A) and (B), may make recommendations to the Administrator of the Federal Aviation Administration if separate or additional rulemaking, policy, or guidance is needed to address aircraft systems information security protection.

(3) RECOMMENDATIONS.—In any recommendation under paragraph (2)(C), the working group shall identify a cost-effective and technology-neutral approach and incorporate voluntary consensus standards and best practices and international practices to the fullest extent possible.

(4) REPORT.—

(A) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, and periodically thereafter, the working group shall provide a report to the Administrator of the

Federal Aviation Administration on the findings of the review and any recommendations.

(B) CONGRESS.—The Administrator shall submit to the appropriate committees of Congress a copy of each report provided by the working group.

(5) CLASSIFIED INFORMATION.—Each report submitted under this subsection shall be in unclassified form, but may include a classified annex.

(c) CYBERSECURITY IMPLEMENTATION PROGRESS.—The Administrator of the Federal Aviation Administration shall—

(1) not later than 90 days after the date of enactment of this Act, and periodically thereafter until the completion date, provide to the appropriate committees of Congress a briefing on the actions the Administrator has taken to improve information security management, including the steps taken to implement subsections (a), (b) and (c) and all of the issues and open recommendations identified in cybersecurity audit reports issued in 2014 and 2015 by the Inspector General of the Department of Transportation and the Government Accountability Office; and

(2) not later than 1 year after the date of enactment of this Act, issue a final report to the appropriate committees of Congress on the steps taken to improve information security management, including implementation of subsections (a), (b) and (c) and all of the issues and open recommendations identified in the cybersecurity audit reports issued in 2014 and 2015 by the Inspector General of the Department of Transportation and the Government Accountability Office.