U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable John Thune
Chairman, Committee on Commerce,
Science and Transportation
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Shuster and Smith, Senator Nelson, Congresswoman Johnson, and Congressman DeFazio.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable Bill Nelson
Committee on Commerce, Science
and Transportation
United States Senate
Washington, DC 20515

Dear Senator Nelson:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Thune, Shuster, and Smith; Congresswoman Johnson; and Congressman DeFazio.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable Bill Shuster
Chairman, Committee on
Transportation and Infrastructure
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Thune and Smith, Senator Nelson, Congresswoman Johnson, and Congressman DeFazio.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable Peter A. DeFazio
Ranking Member, Committee on Transportation
and Infrastructure
House of Representatives
Washington, DC 20515

Dear Congressman DeFazio:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Thune, Shuster, and Smith; Senator Nelson; and Congresswoman Johnson.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable Lamar Smith
Chairman, Committee on
Science, Space, and Technology,
House of Representatives
Washington, DC 20510

Dear Mr. Chairman:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Shuster and Thune, Senator Nelson, Congresswoman Johnson, and Congressman DeFazio.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

June 19, 2017

The Honorable Eddie Bernice Johnson
Ranking Member, Committee on Science,
Space, and Technology,
House of Representatives
Washington, DC 20515

Dear Congresswoman Johnson:

As required by the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, Section 2111, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to provide a report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for FAA information and FAA information systems within set timeframes, and an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

Identical letters have been sent to Chairmen Shuster, Thune, and Smith; Senator Nelson; and Congressman DeFazio.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

Introduction

In accordance with Section 2111(d), Aviation Cybersecurity, of the FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, the Federal Aviation Administration (FAA) is required to transmit a report on (1) a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's (NIST) latest revisions to information security guidance for FAA information and information systems within set timeframes, and (2) an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes. The FAA, in consultation with NIST, is working on several initiatives to ensure that FAA information and information systems meet the requirements of the current NIST standards and guidance in accordance with the FAA mission.

FAA Cybersecurity Initiatives Under Section 2111(d)

Initiative 1: FAA Security Authorization Handbook

The FAA Security Authorization Handbook, referred to as the "FAA Handbook", incorporates U.S. Department of Transportation's (DOT) Departmental Cybersecurity Policy Order 1351.37, DOT Departmental Cybersecurity Compendium Policy, as well as NIST, Federal Information Security Management Act (FISMA), and Office of Management and Budget (OMB) requirements into the FAA security authorization process. The security authorization process applies the Risk Management Framework from NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. The FAA Handbook, maintained by the FAA Office of Information Security and Privacy Service, is updated annually in accordance with DOT Cybersecurity Policy, including OMB Circular A-130, FISMA, and associated NIST Special Publications.

The FAA Handbook applies to all FAA information systems and is required to be followed throughout a system's lifecycle, including the system's initial authorization. It provides procedures, processes and guidelines based on current DOT policies and NIST publications to meet the requirements for initial security authorization, annual assessment, and continuous monitoring. The security authorization process includes conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. As part of the new Risk Executive function, carried out by the FAA Cybersecurity Steering Committee, high value risks and risk acceptance decisions are reviewed by the Committee on a monthly basis to ensure cognizance of the enterprise risk state.

Initiative 2: DOT Cybersecurity Assessment and Management Tool

The DOT Cybersecurity Assessment and Management (CSAM) tool is used to leverage guidance from NIST, OMB, and industry best practices. This tool is also used to document and manage system vulnerabilities and weaknesses as defined in resultant Plan of Action and Milestones (POA&Ms). POA&Ms are created in CSAM to report weaknesses identified in the information systems and corresponding corrective action plans. The FAA is currently performing an analysis

of all open POA&Ms within CSAM to identify and evaluate potential enterprise solutions to address FAA information system security requirements.

Initiative 3: FAA Information Security and Privacy Program & Policy Order 1370.121

In order to properly assign roles to personnel within the organization, the FAA has published FAA Information Security and Privacy Program & Policy Order 1370.121 to align with DOT Departmental Cybersecurity Policy Order 1351.37, which specifies the NIST roles and responsibilities within the context of DOT.

Initiative 4: FAA Acquisition Management System

The FAA is updating contract clauses in the Acquisition Management System for new Agency acquisitions to ensure that contractor provided systems meet current Federal and FAA information system security requirements. The FAA is also developing strategies to apply current NIST standards and guidance to systems under existing contracts.

Summary

The FAA is committed to advancing its cybersecurity capabilities and efforts to maintain protection of FAA information, FAA information systems, and the FAA mission. We continue to improve implementation and alignment of NIST standards and guidelines across the Agency, including adoption of the latest revisions, with our information security controls, policies, and processes. As standards and guidelines are revised in response to evolving cyber threats, the FAA will work to maintain currency when designing, implementing, and assessing information systems.

The FAA Handbook and FAA Order 1370.121 both articulate that the FAA follows NIST guidance in the securing of FAA information and information systems, maintains compliance with NIST standards and guidelines, and implements NIST revisions within the set timeframes.