The Federal Aviation Administration (FAA) manages our Nation’s air traffic control operations through a vast network of information systems and air traffic control facilities. Cyber-based threats—from both internal and external sources—are rapidly evolving and could threaten the connectivity of a complex aviation infrastructure. Furthermore, FAA’s current modernization efforts increasingly rely on integrated information systems, distribution of information, and satellite-based technologies, and as a result, may put the air-traffic control system at greater risk for compromise.

In April 2017, the Chairman and Ranking Members of the U.S. House Committee on Transportation and Infrastructure and the Chairman and Ranking Member of the subcommittee on Aviation requested that we assess FAA’s progress in addressing components of Section 2111 of the FAA Extension, Safety, and Security Act of 2016.\(^1\) Section 2111 of the act establishes requirements for FAA to enhance the cybersecurity of the National Airspace System (NAS) with an approach that considers the interactions and interdependencies of the NAS’s components. Accordingly, our audit objective is to assess FAA’s progress in meeting the requirements of Section 2111 of the FAA Extension, Safety, and Security Act of 2016.

\(^1\) Public Law 114-190.
We plan to begin our audit in July 2017, and will contact your audit liaison to schedule an entrance conference. If you have any questions, please contact me at 202-366-0500, or Nathan Custer, Program Director, at 202-366-5540.

#

cc: FAA Audit Liaison, AAE
    DOT Audit Liaison, M-1