



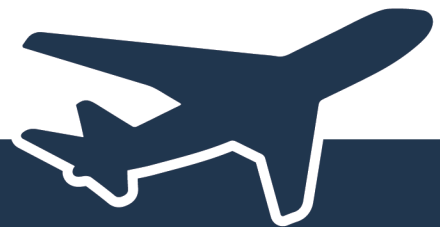
U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

**FAA and Its Partner Agencies Have Begun
Work on the Aviation Cyber Initiative and
Are Implementing Priorities**

FAA

Report No. AV2020043

September 2, 2020





FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities

Requested by the House Committee on Transportation and Infrastructure

Federal Aviation Administration | AV2020043 | September 2, 2020

What We Looked At

FAA oversees the safety of civil aviation through a complex network of information systems at air traffic control facilities. Cyber-based threats are rapidly evolving and may put air traffic control systems at risk for compromise. The FAA Extension, Safety, and Security Act of 2016 directs FAA to develop a comprehensive, strategic framework to reduce cybersecurity risks to civil aviation. Part of FAA's efforts to implement this framework involves coordination and collaboration on aviation cybersecurity with the Departments of Homeland Security (DHS) and Defense (DOD) through the Aviation Cyber Initiative (ACI). The former Chairman of the House Committee on Transportation and Infrastructure requested that we examine FAA's roles, responsibilities, and actions as an ACI member. Specifically, we assessed ACI's progress in achieving its mission.

What We Found

For 3 years, FAA and its ACI partners have been providing regular updates to Federal agencies on their work, and are collaborating with Federal and aviation industry cybersecurity stakeholders. In May 2019, the Secretaries of DHS, DOD, and the Department of Transportation (DOT) finalized the approval of a charter that outlines ACI's objectives. As DOT's representative, FAA is an ACI co-chair with DHS and DOD. The co-chairs report to an Executive Committee of senior Agency executives. At the first ACI Executive Committee meeting in May 2019, 10 priorities were set for 2019 and 2020. ACI has implemented three of these priorities and they are on-going. ACI has also initiated work on the remaining seven. However, ACI has not developed mechanisms to monitor and evaluate results for meeting milestones and timetables for its priorities. ACI lacks an integrated budget and dedicated resources. As a result, FAA and its ACI partners face challenges in achieving its priorities; these challenges could inhibit FAA's ability to develop a comprehensive and strategic framework for cybersecurity.

Our Recommendations

To enhance FAA's progress in achieving ACI's mission, we made one recommendation. FAA concurred with our recommendation.

Contents


| | |
|---|----|
| Memorandum | 1 |
| Results in Brief | 3 |
| Background | 4 |
| FAA and Its ACI Partners Have Begun To Collaborate, Have Finalized ACI's Charter, and Are Implementing Priorities | 5 |
| Conclusion | 9 |
| Recommendations | 9 |
| Agency Comments and OIG Response | 9 |
| Actions Required | 10 |
| Exhibit A. Scope and Methodology | 11 |
| Exhibit B. Organizations Visited or Contacted | 12 |
| Exhibit C. List of Acronyms | 14 |
| Exhibit D. Major Contributors to This Report | 15 |
| Appendix. Agency Comments | 16 |



Memorandum

Date: September 2, 2020

Subject: INFORMATION: FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities | Report No. AV2020043

From: Matthew E. Hampton 
Assistant Inspector General for Aviation Audits

To: Federal Aviation Administrator

The Federal Aviation Administration (FAA) oversees the safety of civil aviation—including aircraft, aircraft systems, and air traffic management—through a complex network of information systems at air traffic control facilities. Rapidly evolving cyber-based threats¹ may put air traffic management systems at risk for compromise as they become more integrated through FAA's implementation of the Next Generation Air Transportation System (NextGen)—programs, systems, and procedures that provide new capabilities for air traffic management.

The FAA Extension, Safety, and Security Act of 2016² directs FAA to develop a comprehensive, strategic framework of principles and policies to reduce cybersecurity risks to civil aviation. In its development of these principles and policies, FAA is to take into consideration the interactions and interdependence of civil aviation components. Part of FAA's efforts to implement this framework involves collaboration and coordination on aviation cybersecurity with the Departments of Homeland Security (DHS) and Defense (DOD) through the Aviation Cyber Initiative (ACI). ACI's mission is to reduce cybersecurity risks and improve resiliency to support safe and secure operation of aircraft, aviation systems, and air traffic management.

Rep. Bill Shuster, then Chairman of the House Committee on Transportation and Infrastructure, requested that we examine FAA's participation with ACI. Accordingly, our audit objective was to examine FAA's roles, responsibilities, and actions as an ACI member, especially those pertaining to its authority over civil

¹ According to the Government Accountability Office, a cyber-based threat can be either intentional or unintentional and come from a variety of sources, including criminals, foreign nations, and terrorists (*see FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221 (2015)).

² Pub. L. No. 114-190.

aviation and air traffic management. Specifically, we assessed ACI's progress on achieving its mission.

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the entities we visited or contacted.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1987.

cc: The Secretary
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

Results in Brief

FAA and its ACI partners have begun collaboration, finalized ACI's charter, and are implementing priorities.

For 3 years, FAA and its ACI partners have been providing regular updates to Federal agencies on their work, and are collaborating with Federal and aviation industry cybersecurity stakeholders. For example, in March 2019, ACI initiated community of interest meetings with representatives from Federal agencies and industry to share information on cybersecurity issues. In May 2019, the Secretaries of DHS, DOD, and the Department of Transportation (DOT) finalized the approval of ACI's charter which outlines the group's objectives. FAA, as DOT's ACI representative, is a co-chair along with DHS and DOD. The co-chairs report to ACI's Executive Committee made up of senior Agency executives. At the first ACI Executive Committee meeting in May 2019, 10 priorities were set for 2019 and 2020. ACI has implemented three of these priorities and they are on-going. ACI has also begun work on the remaining seven. One initiated priority—scheduled for completion in the last quarter of 2020³—involves a Federal agency collaboration to reduce risks to operational security of military aircraft using FAA's satellite-based surveillance system. Two other initiated priorities—a communication plan and the establishment of internal working groups—are in final development and scheduled for completion by the second quarter of 2020. The Government Accountability Office (GAO) outlines practices—such as defining common outcomes and establishing roles and responsibilities—that can enhance and sustain Federal collaboration efforts; ACI has accomplished these practices. However, ACI has not developed mechanisms to monitor and evaluate results, especially for meeting milestones and timetables. Since ACI lacks an integrated budget and dedicated resources, FAA and its ACI partners face challenges in achieving its priorities. The lack of dedicated resources could also inhibit FAA's ability to develop a comprehensive and strategic framework to reduce cybersecurity risks to air traffic management as required by the FAA Extension, Safety, and Security Act of 2016.

We made one recommendation to help improve FAA's coordination and collaboration with its partners to achieve ACI's priorities. FAA concurs with this recommendation.

³ In calendar year 2020.

Background

In 2017, the National Security Council directed the Office of the Director of National Intelligence, in association with other Federal agencies, to update the National Strategy for Aviation Security (NSAS).⁴ Originally drafted in 2007, the NSAS calls for an integrated approach to address aviation security challenges. The updated NSAS expands this approach to include the Aviation Ecosystem—a network of airports, airlines, aircraft (manned and unmanned), airlift, and aviation actors—the people who operate, maintain, and use the Ecosystem, and aviation management, regulators, operation managers, and administrators. In December 2018, the President signed the updated NSAS.⁵

According to the updated NSAS, DHS, FAA, and DOD are to share responsibilities for coordinating aviation infrastructure security activities. The NSAS also reflects FAA's responsibility for safety oversight for much of the Aviation Ecosystem, and that DHS must consult with FAA before taking action on aviation safety, air carrier operations, aircraft airworthiness, or use of airspace.

Prior to the updating of the NSAS, in 2016, a multi-agency team known as the Commercial Aviation Cybersecurity Task Force was established to focus on identifying aircraft system cybersecurity vulnerabilities. The task force members included DHS, FAA, DOD, and the Federal Bureau of Investigation. The members created a charter that included definitions of the Agencies' roles and an outline of mission and supporting objectives, with DHS as the lead agency.

According to the DHS co-chair, to meet the new NSAS's requirements, representatives of DHS, FAA, and DOD from the 2016 task force created what is now known as ACI. Between 2017 and 2019, ACI worked to establish a new charter to focus on the NSAS's direction to integrate aviation cybersecurity through the Aviation Ecosystem, and to emphasize a collaborative approach to aviation cybersecurity.

⁴ DHS, *National Strategy for Aviation Security* (March 2007), available at <https://www.dhs.gov/sites/default/files/publications/nspd-47.pdf>.

⁵ See <https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf>.

FAA and Its ACI Partners Have Begun To Collaborate, Have Finalized ACI's Charter, and Are Implementing Priorities

FAA and its ACI partners communicate with external groups, have begun collaboration on cybersecurity risk reduction, finalized ACI's charter, and set 10 priorities for 2019 and 2020. ACI has implemented three of these priorities with activities on-going, and is working on implementing the rest.

FAA and Its ACI Partners Communicate with External Groups, Have Begun To Collaborate on Cybersecurity Risk Reduction, and Have Finalized ACI's Charter

Since 2017, FAA and its ACI partners have been communicating with external groups on its status. For example, they provide quarterly briefings to the National Security Council on ACI's progress. Since early 2017, the group has also provided quarterly briefings to FAA's NextGen Executive Board on its development progress and member Agencies' activities in cybersecurity.

Also in 2017, ACI began its work as a collaborative forum on cybersecurity risk reduction. The group engages with existing cybersecurity working groups sponsored by Federal agencies and industry—including those at DOD, the Aviation Government Coordinating Council, and the Aerospace Industries Association—to share information on cybersecurity strategies, issues, and policies.

In March 2019, ACI began meeting with Federal agencies and industry to discuss cybersecurity issues, events, and activities, and share information. Referred to as "community of interest" meetings, participants include representatives from Agencies such as the National Aeronautics and Space Administration and the Department of Commerce, and industry trade associations such as Airlines for America and the Air Line Pilots Association. These meetings occur every other month.

In May 2019, the Secretaries of DHS, DOD, and DOT finalized the approval of ACI's new charter. To comply with the NSAS's guidance, the charter sets ACI's focus on the integration of aviation cybersecurity through all facets of aviation. It

also calls for ACI to act as a forum for collaboration and coordination on cybersecurity risk reduction activities. The charter outlines ACI's objectives, which are to (1) identify, assess, and analyze cyber threats, vulnerabilities, and consequences within the Aviation Ecosystem through research, development, testing, and evaluation initiatives; (2) engage with Aviation Ecosystem stakeholders on activities for reducing cyber risks; and (3) seek opportunities for improving aviation cybersecurity and risk mitigation strategies.

The charter establishes DHS, DOD, and DOT's representatives—DOT's is FAA—as co-chairs in ACI's work to improve collaboration and promote interagency consensus. The charter also establishes an Executive Committee made up of a senior official from each member Agency. FAA's Deputy Administrator represents DOT on the Committee. The Executive Committee is responsible for guiding and supporting ACI's objectives and ensuring that the outreach efforts, interests, authorities, policies, and missions of ACI's member Agencies are maintained and coordinated. Twice a year, the member Agencies brief the Executive Committee on the status of ACI's work, and discuss how ACI will move forward.

ACI lacks an integrated budget with its partner Agencies and its only full-time staff are the three co-chairs. However, FAA provides ACI with technical support, cybersecurity knowledge, and expertise from its various lines of business.

FAA and its ACI Partners Have Agreed on Priorities and Are Implementing Them

ACI's partner Agencies and the Executive Committee held their first meeting in May 2019, and agreed on 10 priorities for ACI for 2019 and 2020. At the second Executive Committee meeting in November 2019, ACI established timeframes for completing each priority.

ACI has implemented three priorities—community of interest meetings, cybersecurity trainings and assessments for airport authorities, and an ACI website portal—and they are on-going. ACI conducted the first community of interest meeting in March 2019, and eight more as of April 2020. In 2019, ACI conducted WiFi assessment trainings at four airports and cybersecurity assessments at two. In March 2019, ACI established the structure for its website portal, and in November 2019, formalized access controls to the portal.

ACI is in the process of implementing the remaining seven priorities. One—a collaboration sponsored by DOD and endorsed by ACI partner Agencies to mitigate cybersecurity risks to the operational security of military aircraft using

FAA’s satellite-based surveillance system⁶—is scheduled for completion in the fourth quarter of 2020. Another priority—a summit for Government and industry aviation stakeholders—is scheduled to occur in the fourth quarter of 2020. See the table for the status of ACI’s implementation of these 10 priorities.

Table. Status, as of April 2020, of ACI’s 10 Priorities for 2019 and 2020

| Priority | Status | Completion Date |
|--|-------------|--|
| Establish working groups | Initiated | Second quarter 2020 |
| Develop communication plan | Initiated | Second quarter 2020 |
| Hold Community of Interest meetings | Implemented | Activities are on-going |
| Activate ACI website | Implemented | Activities are on-going |
| Develop a scenario-based legal and policy analysis of aviation cybersecurity | Initiated | Third quarter 2020 |
| Revitalize research and development initiatives | Initiated | Fourth quarter 2020 |
| Establish a cybersecurity risk reduction project for satellite-based surveillance | Initiated | Fourth quarter 2020 |
| Develop and conduct cybersecurity training and assessments for airport authorities | Implemented | Activities are on-going |
| Hold ACI summit | Initiated | Fourth quarter 2020 |
| Develop an aviation cybersecurity event for the National Level Exercise 2020 | Initiated | Originally scheduled for March 2020, then rescheduled for second quarter 2020. |

Source: ACI and OIG analysis.

Two initiated but incomplete priorities are the establishment of a communication plan and internal working groups. The communication plan, called for in ACI’s charter, will describe how ACI will communicate the results of its work—including test results, reports, assessments, and other work—to Federal and aviation industry cybersecurity stakeholders. The plan will ensure that communications on cybersecurity are accurate, consistent, and properly coordinated within and among involved ACI Agencies. According to FAA’s co-chair, in January 2020, ACI circulated a draft plan for comments during an interagency workshop. The draft is currently in the final approval process at each Agency.

⁶ The Automatic Dependent Surveillance–Broadcast system.

Because ACI does not have an integrated budget or dedicated staff, the co-chairs decided on a working group structure to conduct ACI's work. They plan on 11 working groups covering cybersecurity areas such as policy and standards, unmanned aircraft systems, and risk mitigation. Working group membership will consist of personnel from Federal agencies and industry.

In October 2019, ACI completed guidance for its working groups, which identifies "lines of effort" and supporting objectives. These lines of effort include: (1) identifying and addressing cybersecurity risks; (2) improving cybersecurity resilience; (3) improving aviation cybersecurity information sharing, coordination, and collaboration; and (4) ensuring ACI's on-going effectiveness and value.

Of ACI's 11 planned working groups, 9 have identified leads, 7 are conducting meetings, and 5 have established objectives. For example, the testing and assessment working group is establishing a list of projects to generate awareness of its efforts. The research and development working group has established a subgroup to conduct research on the protection of systems from unauthorized software changes caused by cybersecurity attacks. According to ACI, all 11 working groups will begin work by the end of the second quarter of 2020.

ACI has initiated work on three other priorities, including a legal and policy gap analysis and an aviation cybersecurity event for the National Level Exercise 2020.⁷ The National Security Council asked ACI to develop three aviation cybersecurity scenarios to identify gaps, overlaps, and conflicts in laws and policies that impact Agency cybersecurity roles and responsibilities. ACI plans to develop table top exercises that participants can use to simulate scenarios to develop methods to address identified gaps. These exercises will form the basis for the aviation cybersecurity event for National Level Exercise 2020. The Exercise has been cancelled for 2020 due to the pandemic, but on June 30, ACI held a table top exercise through a distance communications application.

According to GAO,⁸ certain practices enhance and sustain collaboration among Federal agencies, including definition and articulation of common outcomes, agreement on agency roles and responsibilities, and development of mechanisms to monitor, evaluate, and report the results of collaborative efforts. In ACI's charter, the co-chairs have defined a common outcome for their efforts and agreed on Agency roles and responsibilities. However, ACI's mechanisms for monitoring, evaluating, and reporting on results are still in development. ACI

⁷ The National Level Exercise is a biennial Federal Government-sponsored event where entities can test operational capabilities and evaluate policies and plans against scenarios such as natural disasters and man-made attacks. The 2020 event focuses on cybersecurity.

⁸ GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (2012); *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (2005).

officials stated that while they have established milestones and completion dates for its priorities, they could not provide a plan for remaining on schedule.

Due to its lack of an integrated budget and dedicated resources, ACI faces challenges achieving its priorities. The working groups are primarily responsible for implementing the remaining priorities but may face difficulties meeting scheduled milestones because they must rely on volunteer staff. These resource limitations could also impact FAA's development of a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to air traffic management, as mandated in the FAA Extension, Safety, and Security Act of 2016.

Conclusion

ACI is a key mechanism for facilitating collaboration and coordination of cybersecurity issues among Federal agencies and the aviation industry. Now, 3 years after its establishment, ACI has set its priorities and started to identify cybersecurity risks. FAA and its ACI partners' work to identify and mitigate cybersecurity vulnerabilities will help reduce the possible impact these vulnerabilities have on the National Airspace System and aviation stakeholders.

Recommendations

To enhance FAA's progress in achieving ACI's mission, we recommend that the Federal Aviation Administrator:

1. In consultation with its ACI partners, identify the resources needed to meet the current schedule for achieving ACI's remaining priorities, and how they should be allocated. Revise the current schedule as necessary to reflect the resources that are available.

Agency Comments and OIG Response

We provided FAA with our draft report on July 10, 2020, and received its formal response on August 4, 2020. FAA's response is included in its entirety as an appendix to this report. FAA also provided technical comments which we incorporated into this report where appropriate. In its management response, FAA concurred with our recommendation as written and provided proposed a completion date.

Actions Required

We consider our recommendation resolved but open pending FAA's completion of planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between May 2019, and July 2020, in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Rep. Bill Shuster, then Chairman of the House Committee on Transportation and Infrastructure, requested that we examine FAA's participation with ACI. Accordingly, our audit objective was to examine FAA's roles, responsibilities, and actions as an ACI member, especially those that pertain to its authority over civil aviation and air traffic management. Specifically, we assessed ACI's progress on achieving its mission.

We collected and analyzed relevant Federal cybersecurity guidance and ACI documents. We analyzed the recently updated NSAS directed by the National Security Presidential Directive 47/Homeland Security Presidential Directive 16, and its supporting plans. We analyzed the ACI charter, approved in May 2019, and working group guidance issued in October 2019. We reviewed notes from ACI community of interest meetings and from the ACI Executive Committee meetings in May and November 2019. We reviewed the FAA Reauthorization Act of 2018⁹ for information on congressional direction for cybersecurity activities. We also reviewed GAO's interagency collaboration mechanisms for multi-agency coordination best practices.

We interviewed the ACI co-chairs representing FAA, DOD, and DHS. We interviewed representatives from private sector and Government cybersecurity working groups and organizations who have coordinated with FAA and ACI on cybersecurity issues. We interviewed FAA officials who conduct FAA cybersecurity activities and coordinate with ACI. These offices include the Air Traffic Organization, the Office of Airports, the Office of National Security Programs and Incident Response, the Office of Finance and Management, and the Next Generation Air Transportation System staff office. We also interviewed officials from DHS's Science and Technology directorate who coordinate with ACI on future activities.

⁹ Pub. L. No. 115-254.

Exhibit B. Organizations Visited or Contacted

Federal Aviation Administration Headquarters

Office of NextGen

- NextGen Collaboration and Messaging Office
- Office of the Chief Scientist for NextGen
- Air Traffic Systems Testing and Evaluation Services Division

Air Traffic Organization

- Technical Operations, National Airspace System Information Security Group

Office of Airports

- Office of the Associate Administrator for Airports

Office of Security and Hazardous Materials Safety

- Office of National Security Programs and Incident Response

Office of Finance and Management

- Office of Information Security and Privacy

Other Organizations

Aviation Cyber Initiative Co-Chairs from FAA, DHS, and DOD

Cybersecurity Working Groups

- Aerospace Industries Association
- Aircraft Cyber Threats, Department of the Air Force, DOD
- Aviation Government Coordinating Council
- Policy Board on Federal Aviation, Department of the Air Force, DOD

Aviation Information Sharing and Analysis Center

Science and Technology Directorate, Cybersecurity Division, DHS

White House Office of the Director of National Intelligence, National Aviation
Intelligence Integration Office

Exhibit C. List of Acronyms

| | |
|---------|---|
| ACI | Aviation Cyber Initiative |
| DHS | U.S. Department of Homeland Security |
| DOD | U.S. Department of Defense |
| DOT | U.S. Department of Transportation |
| FAA | Federal Aviation Administration |
| GAO | Government Accountability Office |
| NextGen | Next Generation Air Transportation System |
| NSAS | National Strategy for Aviation Security |
| OIG | Office of Inspector General |

Exhibit D. Major Contributors to This Report

NATHAN CUSTER

ARNETT SANDERS

KIESHA MCMILLAN

JAMES MULLEN

MI HWA BUTTON

TAMARIA KELLY

SUSAN NEILL

AMY BERKS

PROGRAM DIRECTOR

PROJECT MANAGER

SENIOR AUDITOR

INFORMATION SYSTEMS SPECIALIST

ANALYST

ANALYST

WRITER-EDITOR

DEPUTY SENIOR COUNSEL

Appendix. Agency Comments



Federal Aviation Administration

Memorandum

Date: August 4, 2020

To: Matthew E. Hampton, Assistant Inspector General for Aviation Audits

From: H. Clayton Foushee, Director, Office of Audit and Evaluation, AAE-1

Subject: FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities

The national airspace system (NAS) is becoming increasingly reliant upon information technology. Establishing a framework to coordinate with other government agencies and NAS stakeholders is critical to defending the NAS against cyber-attacks. Accordingly, the Federal Aviation Administration (FAA) serves as a tri-chair of the Aviation Cyber Initiative (ACI). The ACI provides a collaborative forum to support the reduction of cyber risks and to improve resilience to promote safe, secure, and efficient operation of aircraft within the NAS. This cybersecurity initiative includes all aspects of the aviation ecosystem, including the components, infrastructure, and operations necessary to support the uninterrupted safe and efficient movement of aircraft. FAA works continuously with other government agencies and aviation system stakeholders to build relationships and coordinate capabilities with the goal of maintaining a state-of-the-art cybersecurity defense.

We concur with the OIG's recommendation that FAA, in consultation with its ACI partners, identify the resources needed to meet the current schedule for achieving ACI's remaining priorities and how those resources should be allocated, and revise the current schedule, as necessary. FAA plans to implement the recommendation by December 31, 2020.

We appreciate the opportunity to respond to the OIG draft report. Please contact H. Clayton Foushee at clay.foushee@faa.gov if you have any questions or require additional information about these comments.

U.S. DOT IG Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

<https://www.oig.dot.gov/hotline>

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590



www.oig.dot.gov