U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

Opportunities Exist To Further Strengthen the Security Controls of FAA's Data Communications Program

FAA

Report No. FI2018059

July 3, 2018

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

Opportunities Exist To Further Strengthen the Security Controls of FAA's Data Communications Program

Self-Initiated

Federal Aviation Administration | FI2018059 | July 3, 2018

What We Looked At

Part of the Federal Aviation Administration's (FAA) efforts to modernize and increase the efficiency of the Nation's aging air traffic system, Data Communications (DataComm) will play an important role in air traffic controller to flight crew communication. Thus, it is critical that FAA incorporate sufficient controls to protect against potential security threats to that communication, including an effective contingency plan to ensure a quick recovery from losses of DataComm availability. Accordingly, we initiated this audit to determine whether (1) FAA is identifying and properly mitigating security risks and (2) FAA's contingency plan is sufficient to limit the effects of DataComm availability losses. We focused on two DataComm systems during our review—the Data Communications Network Service (DCNS) and Tower Data Link Services (TDLS).

What We Found

FAA is identifying—but is not mitigating—security risks in a timely manner. Specifically, two high-impact plans of action and milestones (POA&M) were scheduled to be completed in October 2017. However, as of May 10, 2018, FAA had not mitigated the two security control vulnerabilities. An Agency official stated that FAA is working with a vendor to complete the first POA&M by December 31, 2018, and the second POA&M by March 31, 2019. FAA's contingency plans for DCNS and TDLS are sufficient to limit the effects of DataComm unavailability.

This report is marked For Official Use Only to protect sensitive information exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552. Accordingly, a redacted version of the report has been posted to our website.

Our Recommendation

FAA concurred with our one recommendation to improve DataComm security controls.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: July 3, 2018

Subject: Opportunities Exist To Further Strengthen the Security Controls of FAA's Data Communications Program | Report No. FI2018059

From: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

To: Federal Aviation Administrator

The Federal Aviation Administration's (FAA) Data Communications (DataComm) program is part of the Next Generation Air Transportation System (NextGen) initiative. NextGen is intended to modernize and increase the efficiency of our Nation's aging air traffic system. DataComm will assume a pivotal role in air traffic controller to flight crew communication, contributing significantly to the increased efficiency, capacity, and safety of the National Airspace System (NAS). As of February 2018, DataComm has been implemented in 57 airports, and is fully operational in over 1,100 aircraft. FAA expects to expand the program to seven more airports based on air carrier requests. FAA's successful implementation of DataComm is expected to produce a number of operational benefits, including increased safety, higher controller productivity, greater aircraft fuel savings, and infrastructure support for other NextGen programs and operational improvements.

Given the important role that DataComm will play in communications between controllers and flight crews, it is critical that FAA incorporate sufficient controls to prevent potential security threats from compromising flight data and communications. This includes establishing an effective contingency plan to ensure FAA can quickly recover from an unexpected loss of DataComm availability. Accordingly, we initiated this audit of FAA's information technology (IT) security controls for DataComm. Our audit objectives were to determine whether (1) FAA is identifying and properly mitigating security risks and (2) FAA's

contingency plan is sufficient to limit the effects of DataComm availability losses.[1] We focused on two DataComm systems during our review—the Data Communications Network Service (DCNS) and Tower Data Link Services (TDLS).[2]

To conduct our work, we interviewed officials at the Department of Transportation (DOT) and FAA Headquarters offices in Washington, DC, and the FAA William J. Hughes Technical Center (WJHTC)[3] in Atlantic City, NJ. We conducted site visits at the Memphis, TN, and Louisville, KY, airports, which are two of the three busiest cargo airports in America. They are also hubs for FedEx Corporation (FedEx) and United Parcel Service (UPS), respectively, which were early users of DataComm and helped in the development process. In addition, we issued data calls to FAA and reviewed copies of the Agency's Certification and Accreditation Package documents for the DataComm systems. We conducted our work in accordance with generally accepted Government auditing standards. Exhibit A describes our scope and methodology, exhibit B lists the organizations we contacted or visited, and exhibit C lists the acronyms used in this report.

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) 366-1407 or Abdil Salah, Program Director, at (202) 366-8543.

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

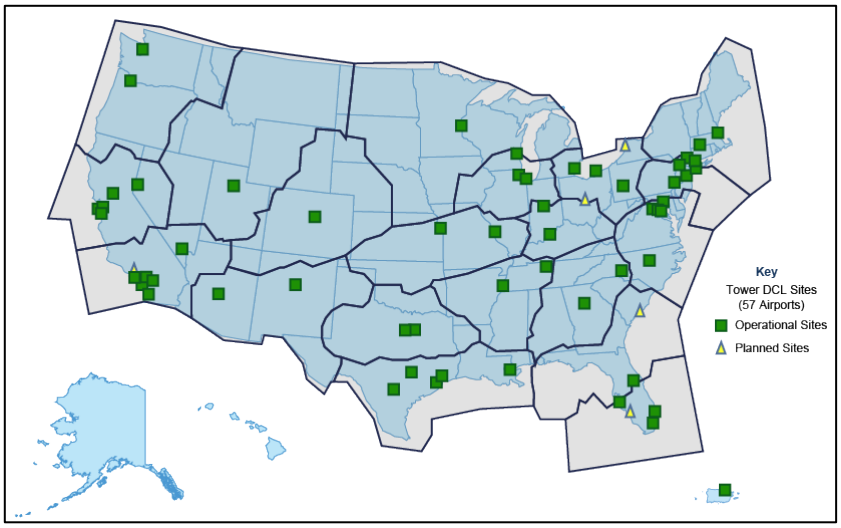
[1] While we reported in 2017—*DOT's Fiscal Year 2018 Top Management Challenges* (OIG Report No. PT2018005), November 15, 2017—that FAA had not been proactive in addressing and closing known security weaknesses, we have not previously performed a security controls audit of the DataComm program.
[2] DCNS, the networking component of the Data Communications Integrated Services (DCIS) program, addresses the data communication between FAA automation systems and aircraft. TDLS provides information to flight deck crews using aeronautical data links from the air traffic control tower.
[3] WJHTC is the Nation's premier air transportation system laboratory, where FAA tests and evaluates DataComm.

Background

DataComm supplements the current voice communication system between air traffic controllers and the aircraft flight deck by enabling precise visual messages and digital instructions to appear on a cockpit display—reducing opportunities for error. Specifically, DataComm allows air traffic controllers to send text-based instructions instead of speaking over a radio. In turn, after reading the instructions, flight crews can acknowledge receipt simply by pushing a button. Instructions can be changed multiple times before an airplane departs. This system also automates communication between air traffic control and airline pilots. DataComm should increase both the accuracy and speed as well as enhance safety by reducing communication errors.

FAA has deployed DataComm at 57 airports (see figure 1), which completes phase 1 of the DataComm Initiative. FAA estimates that DataComm implementation is currently over 2 years ahead of schedule and under budget.[4] Phase 2 will involve adding en route services, such as rerouting aircraft while in flight. Initial en route services are scheduled to start operating in 2019.

Figure 1. Deployment of DataComm as of February 2018



Source: FAA

[4] Future phases of the program will take place after implementation and include the integration of DataComm into the larger En Route Automation Modernization program to increase efficiency and support flight services.

Results in Brief

FAA is identifying security risks but is not mitigating them in a timely manner.

In accordance with Federal and departmental guidelines, FAA has developed plans of action and milestones (POA&M)[5] to assess the potential for security vulnerabilities in DCNS and TDLS. The POA&Ms show that FAA has effectively identified and documented security risks for these DataComm systems. However, while two high-impact POA&Ms were scheduled to be completed in October 2017, as of May 10, 2018, FAA had not mitigated the two security control vulnerabilities. For example, FAA uses certain applications and operating systems that are no longer supported by vendors, but those vulnerabilities had not been remediated by the time we completed our audit field work. IT security control weaknesses that remain unaddressed can compromise the integrity of systems and data. An Agency official stated that FAA is working with a vendor to complete the first POA&M by December 31, 2018, and the second POA&M by March 31, 2019.

FAA's contingency plans for DCNS and TDLS are sufficient to limit the effects of DataComm unavailability.

FAA has developed contingency plans for DCNS and TDLS, in accordance with the National Institute of Standards and Technology's (NIST) guidance for Federal information systems. Our analysis found that these plans are sufficient to limit the effects of a DataComm outage or loss. Furthermore, FAA's contingency plans for the years 2015 and 2016 demonstrate that the Agency is reviewing, testing, and updating the plans annually. As a result, in the event of an outage, FAA will be prepared to restore the DCNS and TDLS systems.

We made one recommendation to help FAA strengthen DataComm's security controls.

[5] POA&Ms help organizations identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems.

FAA Is Identifying Security Risks but Is Not Mitigating Known Security Risks in a Timely Manner

FAA has effectively identified multiple security risks for the two DataComm systems we reviewed, DCNS, and TDLS, and has documented these risks in POA&Ms, in accordance with departmental and Federal guidelines. During our review of FAA's DCNS, we identified two high-impact POA&Ms (SI-02.A and CM07.A.2) that were scheduled to be completed in October 2017. As of May 10, 2018, however, these two security control vulnerabilities had not yet been mitigated. According to the Office of Management and Budget's (OMB) Memorandum M-14-04, agencies can use the POA&M process to focus resources to resolve delays. It also states that agencies cannot postpone corrections to a future budget cycle, but should integrate requirements as weaknesses are identified.

FAA had previously identified these two security deficiencies and wrote the POA&Ms to mitigate the control weaknesses, but did not meet, reduce, or eliminate the vulnerabilities by the planned completion dates. IT security control weaknesses that remain unaddressed for extended periods of time can create unnecessary system exposures that may be exploited by intruders or compromise the availability or integrity of systems and data. An Agency official stated the delay was due to a lack of available funds, and FAA is working with a vendor to complete the first POA&M by December 31, 2018. In addition, funds have been identified for the second POA&M, which the Agency expects to complete by March 31, 2019.

FAA Contingency Plans for DCNS and TDLS Are Sufficient To Limit the Effects of DataComm Unavailability

FAA has contingency test plan and results documents for both DCNS and TDLS. We reviewed the Agency's 2015 and 2016 contingency plans for these two DataComm systems, which show that FAA reviews, tests, and updates the plans annually. Furthermore, our analysis of the documentation and test results provided evidence that contingency plan testing is occurring on an annual basis.

NIST Special Publication 800-34, "Contingency Planning Guide for Federal Information Systems," requires tabletop exercises to be performed for low-impact systems and functional exercises for moderate systems.[6] This testing is required to show that the organization's controls are effective and are evaluated each year. Our analysis of the 2015 and 2016 contingency plans shows that FAA conducts the appropriate types of NIST-required testing for both the low-impact TDLS and the moderate-impact DCNS systems.

FAA's continued commitment to testing increases the likelihood that it will be able to restore the DCNS and TDLS systems in the event of an outage.

Conclusion

The DataComm program is a significant element of FAA's NextGen efforts and is expected to significantly contribute to the increased efficiency, capacity, and safety of the NAS. While FAA is making considerable progress in implementing DataComm, it is vital that the Agency continue to proactively identify security risks and sustain its commitment to contingency testing. In addition, FAA must take prompt action to mitigate identified vulnerabilities by their scheduled completion dates. Otherwise the confidentiality, integrity, and availability of DataComm may remain at risk.

[6] TDLS is listed as a low system and DCNS is listed as a moderate system per NIST's Federal Information Processing Standards Publication 199 (FIPS 199).

Recommendations

To improve Data Communications program security controls, we recommend that the Federal Aviation Administrator:

1. Update and remediate the completion dates in the plans of action and milestones for SI-02.A and CM07.A.2 to ensure that the confidentiality, integrity, and availability of the system are not at risk.

Agency Comments and OIG Response

We provided FAA with our draft report on May 11, 2018, and received its formal response on June 11, 2018. FAA concurred with our one recommendation and provided appropriate actions and completion dates. Accordingly, we consider the recommendation resolved but open pending completion of the planned actions.

Actions Required

We consider recommendation 1 to be resolved but open pending completion of planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between April 2017 and May 2018. We conducted this audit 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.

To analyze how FAA identifies and mitigates security risk, we interviewed DataComm program officials—system administrators and users—and subject matter experts and collected and reviewed security documentation for two DataComm systems currently in operation, DCNS and TDLS. We did not review the En Route Automation Modernization (ERAM) system since initial en route DataComm services (e.g., rerouting aircraft while in flight) in high-altitude airspace are not scheduled to start operating until 2019.

To determine if FAA's contingency plans are sufficient to limit the effects of DataComm availability losses, we reviewed the plans for the DCNS and TDLS systems and the documentation for the annual testing of the contingency plans.

We interviewed officials at DOT and FAA Headquarters offices in Washington, DC, and the FAA William J. Hughes Technical Center in Atlantic City, NJ. We conducted site visits at the Memphis, TN, and Louisville, KY, airports, which are two of the three busiest cargo airports in America. They are also hubs for FedEx and UPS, respectively, which were early users of DataComm and helped in the development process. We met with and interviewed officials from these companies as well. We issued data calls to FAA and obtained and reviewed copies of the Agency's Security Authorization Package documents for DCNS and TDLS.

Exhibit B. Organizations Visited or Contacted

FAA Facilities

FAA Headquarters, Washington, DC

FAA William J. Hughes Technical Center, Atlantic City, NJ

FAA facility at Louisville International Airport, KY

FAA facility at Memphis International Airport, TN

Other Organizations

FedEx, Memphis, TN

United Parcel Service, Louisville, KY

Exhibit C. List of Acronyms

DataComm	Data Communications Program
DCIS	Data Communications Integrated Services
DCNS	Data Communications Network Service
DOT	Department of Transportation
ERAM	En Route Automation Modernization
FAA	Federal Aviation Administration
FedEx	FedEx Corporation
IT	Information technology
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of action and milestones
TDLS	Tower Data Link Services
UPS	United Parcel Service
WJHTC	FAA William J. Hughes Technical Center

Exhibit D. Major Contributors to This Report

ABDIL **SALAH**	PROGRAM DIRECTOR
JAMES **MALLOW**	PROJECT MANAGER
JASON **MOTT**	INFORMATION TECHNOLOGY SYSTEMS SPECIALIST
ANTIONE **SEARCY**	INFORMATION TECHNOLOGY SYSTEMS SPECIALIST
NILESHKUMAR **PATEL**	INFORMATION TECHNOLOGY SYSTEMS SPECIALIST
JAMES **MULLEN**	INFORMATION TECHNOLOGY SYSTEMS SPECIALIST
AUDRE **AZUOLAS**	WRITER-EDITOR
JANE **LUSAKA**	WRITER-EDITOR
PETRA **SWARTZLANDER**	SENIOR STATISTICIAN

Appendix. Agency Comments

Federal Aviation Administration

Memorandum

Date: June 11, 2018

To: Louis C. King, Assistant Inspector General for Financial and Information Technology Audits

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

Subject: Federal Aviation Administration's (FAA) Response to Office of Inspector General (OIG) Draft Report: Opportunities Exist to Further Strengthen the Security Controls of FAA's Data Communications Program

The FAA's Data Communications (Data Comm) program is a vital component of the Next Generation Air Transportation System (NextGen). Data Comm services enhance safety by reducing communication errors, increase productivity by reducing communication time between controllers and pilots, and increase airspace capacity and efficiency while reducing delays and fuel burn. As of May 2018, Data Comm has been implemented successfully at 60 airports, ahead of schedule, and the FAA continues to work on expanding Data Comm capabilities throughout the National Airspace System. The system is expanding to the en-route domain beginning in 2019.

The FAA concurs with the recommendation as written and plans to implement the recommendation by March 31, 2019.

We appreciate this opportunity to respond to the OIG draft report. Please contact H. Clayton Foushee at (202) 267-9000 if you have any questions or require additional information about these comments.

U.S. DOT OIG 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