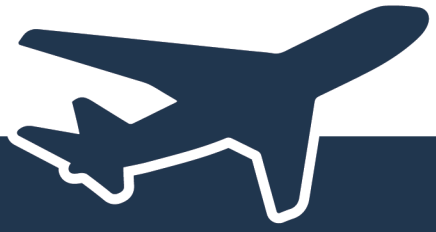
U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

FAA Lacks Sufficient Security Controls and Contingency Planning for Its DroneZone System



FAA

Report No. IT2020027

April 15, 2020

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

FAA Lacks Sufficient Security Controls and Contingency Planning for Its DroneZone System

Self-initiated

Federal Aviation Administration | IT2020027 | April 15, 2020

What We Looked At

In 2012, Congress directed the Federal Aviation Administration (FAA) to develop a plan for the safe integration of unmanned aircraft systems (UAS)—also known as drones—into the National Airspace System. As part of its integration and oversight of UAS, FAA compiles data in its UAS registration service—known as FAA DroneZone—as well as in its Low Altitude Authorization and Notification Capability (LAANC), an automated system that authorizes registered UAS users to fly their drones near airports. Both DroneZone and LAANC are cloud-based systems that contain sensitive data provided by the general public, including personally identifiable information (PII). We initiated this audit to determine whether FAA's UAS registration system has the proper security controls and recovery procedures in place. Our audit objectives were to (1) assess the effectiveness of FAA's UAS registration system security controls, including controls to protect PII, and (2) determine whether FAA's contingency planning limits the effects caused by the loss of DroneZone during disruptions of service.

What We Found

FAA has not effectively ensured that DroneZone and LAANC have adequate security—including privacy—controls. For example, FAA has continued to authorize DroneZone operations without conducting a comprehensive assessment of its security controls since it first began to operate the system in 2015. In addition, FAA's inadequate monitoring of security controls and use of unauthorized cloud systems increases the risk of the systems being compromised. Furthermore, FAA could not demonstrate that 24 of 26 privacy controls were assessed to protect 1.5 million DroneZone users' PII. We also found that FAA's contingency planning does not adequately limit the effects caused by a potential disruption of services. Finally, FAA does not have sufficient controls for handling backups and off-site storage to ensure continuous operations and maintain data availability.

Our Recommendations

FAA concurred with all 13 of our recommendations to improve the security of the DroneZone and LAANC systems and privacy of user information.

Contents

Memorandum 1

Results in Brief 3

Background 4

FAA Has Not Effectively Ensured That DroneZone and LAANC Have Adequate Security and Privacy Controls 6

FAA Contingency Planning Does Not Adequately Limit the Effects Caused by a Potential Disruption of Services 14

Conclusion 17

Recommendations 17

Agency Comments and OIG Response 19

Actions Required 19

Exhibit A. Scope and Methodology 20

Exhibit B. Organizations Visited or Contacted 21

Exhibit C. List of Acronyms 22

Exhibit D. Major Contributors to This Report 23

Appendix. Agency Comments 24

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: April 15, 2020

Subject: ACTION: FAA Lacks Sufficient Security Controls and Contingency Planning for Its DroneZone System | Report No. IT2020027

From: Kevin Dorsey
Acting Assistant Inspector General for Information Technology Audits

To: Federal Aviation Administrator

In 2012, Congress directed the Federal Aviation Administration (FAA) to develop a plan for the safe integration of unmanned aircraft systems (UAS)—also known as drones—into the National Airspace System (NAS).[1] To handle integration of small UAS[2] into the NAS, FAA initially used a paper registration process, which became inefficient as a result of increased small UAS sales. On December 21, 2015, the Agency launched a streamlined and simple web-based process for the registration of small unmanned aircraft called the small Unmanned Aircraft System Registration Service (sUASRS).[3] On November 24, 2017, the FAA DroneZone portal replaced sUASRS.

DroneZone now also contains information on small UAS accidents and requests for waivers of operating rules. The system interfaces with FAA's Low Altitude Authorization and Notification Capability (LAANC), an automated system that provides authorization for UAS registered users requesting permission to fly their drones within 5 miles of an airport. Both DroneZone and LAANC are hosted in a public cloud[4] and contain personally identifiable information (PII), including name and mailing address, for each person or business required to register a small UAS. Registration costs $5, which can be paid by either credit or debit card, is valid for

[1] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332.
[2] "Small UAS" means a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the NAS (14 CFR § 107.3).
[3] Registration and Marking Requirements for Small Unmanned Aircraft; Final Rule Federal Registry Vol.80 No. 241 December 16, 2015.
[4] Cloud computing is the practice of using remote—rather than local—hardware, software, or other computing services to process data. With a public cloud, all hardware, software, and supporting infrastructure are owned and managed by the cloud provider and open for use by the general public. Users access the public cloud via the internet.

3 years, and then must be renewed. As of December 2019, approximately 1.5 million people were registered in DroneZone.

Because of the volume of sensitive data provided by the general public, as well as the importance of UAS user data to FAA's oversight, we initiated this audit to determine whether FAA's UAS registration system has the proper security controls and recovery procedures in place. Accordingly, our audit objectives were to (1) assess the effectiveness of FAA's UAS registration system security controls,[5] including controls to protect PII, and (2) determine whether FAA's contingency planning limits the effects caused by the loss of DroneZone during disruptions of service.

We conducted our work in accordance with generally accepted Government auditing standards for program audits. Exhibit A details our Scope and Methodology, and exhibit B lists the organizations we visited and contacted. For a list of the acronyms used in this report, see exhibit C.

We appreciate the courtesies and cooperation of Department of Transportation (DOT) representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1518.

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

[5] There are three distinct types of designations related to security controls: system-specific controls, common controls, and hybrid controls.

Results in Brief

FAA has not effectively ensured that DroneZone and LAANC have adequate security—including privacy—controls.

We identified several vulnerabilities in FAA's security control assessment process. For example, FAA has continued to authorize DroneZone and LAANC operations without conducting a comprehensive assessment of their security controls since it first began to operate the systems in 2015. Additionally, DroneZone's fiscal year 2019 System Security Plan (SSP), which details its security controls, had over 100 deficiencies, such as implementation status of controls that could result in internal control gaps (e.g., improper system configuration). In addition, FAA is not adequately monitoring DroneZone and LAANC security controls provided by or inherited from its cloud service provider. For example, the cloud service provider does not patch[6] all of its operating systems, increasing the systems' exposure to outside threats. We also found that the Agency's security official incorrectly selected the wrong control type (common, hybrid, and/or system specific) for 79 LAANC and 20 DroneZone controls inherited from a cloud service provider, which resulted in the controls not being properly assessed and in the system not being properly authorized in 2019. Moreover, these systems were supported by other cloud systems that were not authorized to operate, and therefore FAA could not demonstrate the adequacy of their security controls. FAA security and DOT privacy officials also could not demonstrate that 24 of 26 privacy controls to protect 1.5 million PII records in DroneZone were assessed. In addition, FAA is not currently validating that LAANC's service suppliers, who have access to PII, are compliant with security requirements to protect PII. These weaknesses resulted in part from DroneZone and LAANC security officials (e.g., system owners) not having an adequate understanding of their oversight roles or responsibilities. In aggregate, these issues significantly increase the risk that DroneZone and LAANC will be subject to security compromises.

FAA's contingency planning does not adequately limit the effects caused by a potential disruption of services.

We found that 9 of 23 contingency planning security controls for DroneZone and LAANC had been miscategorized, including one critical control that requires a system owner to provide the capability to restore the system. FAA noted that these controls will need to be reassessed as a part of fiscal year 2020 systems security assessment. Additionally, FAA did not update the DroneZone Information System Contingency Planning (ISCP) and testing documentation annually

[6] Software patches are small pieces of software that are used to correct problems (frequently pertaining to security issues) in operating systems and software programs.

according to departmental policies. FAA also did not ensure the ISCP testing was conducted annually for its cloud service provider and contractor. These deficiencies occurred in part because FAA has not sufficiently trained DroneZone personnel on their roles and responsibilities related to contingency planning. We also found that FAA does not have sufficient controls, as described by the National Institute of Standards and Technology (NIST), for handling backups and off-site storage. Together, these weaknesses significantly hinder FAA's ability to ensure continuous operations of the system and maintain data availability in the event of a disaster or disruption of service.

We are making recommendations to improve the security of the DroneZone and LAANC systems and privacy of user information. We are also making other recommendations to improve FAA security officials' oversight of controls inherited from other FAA lines of business and the Agency's cloud service provider.

Background

The emergence of FAA's DroneZone platform has been a continuous and evolutionary process. Prior to the DroneZone concept, FAA produced several stand-alone capabilities to meet mandated rules and regulations for UAS registration, including the following web-based systems:

- Small UAS Registration System (sUASRS): allowed owners and operators to create an account and register their drones for operation in U.S. airspace.
- Part 107[7] Authorization: collected requests to operate a UAS in the NAS.
- Part 107 UAS Accident System: collected information on small UAS accidents for FAA processing, and allowed UAS operators to submit accident reports.
- Part 107 Waiver System: collected FAA information on small UAS owners and operators who applied for airspace and operational waivers.

DroneZone provides a one-stop system for multiple UAS applications designed for an enhanced user experience. The user need just one login for access to all UAS applications.

[7] Part 107 is the FAA regulation that covers a broad spectrum of commercial uses for drones weighing less than 55 pounds.

DroneZone interfaces with LAANC, a software application that runs in the cloud and was deployed in October 2017. LAANC provides a more streamlined approach than DroneZone's manual process, which can take 30 to 90 days. LAANC "automates" FAA's ability to grant authorizations to commercial UAS operators within controlled airspace and allows individuals using UAS for recreational purposes[8] to notify air traffic managers when their planned operations occur within 5 miles of an airport (controlled airspace). LAANC includes a collaboration between FAA and private UAS Service Suppliers. LAANC is designed to interface with UAS Service Suppliers by exchanging authorization information with the suppliers, allowing the suppliers to supply authorizations and submit operational information back to FAA. According to FAA, LAANC is deployed at 400 air traffic control facilities (covering 600 airports).

Both DroneZone and LAANC are systems used by the public and contain PII. As of December 2019, DroneZone contained names, mailing addresses, and email addresses for approximately 1.5 million registrants. PII in LAANC comes from multiple sources and includes:

- UAS Service Suppliers, third-party providers identified by name, a three-letter code, and negotiated authentication key
- UAS pilot names and contact numbers
- Air traffic controller and manager names and email addresses

DroneZone and LAANC software are hosted by a Federal Risk and Authorization Management Program (FedRAMP)[9]-compliant cloud service provider. The cloud service provider received a FedRAMP Joint Authorization Board Provisional Authorization to Operate for its East/West Public Cloud—most recently granted on November 3, 2017. The cloud service is hosted on a network of remote servers distributed throughout the United States. DroneZone and LAANC operate in the cloud service provider's US-West (Oregon) region.

DroneZone and LAANC are contractor systems managed by the contractor's systems developer. All DroneZone administrators are contractor employees, who manage the system and the host environment. According to FAA officials, the contractor is responsible for developing key security documents for both systems, including SSPs, that identify all required security controls. Additionally, the contractor is responsible for managing vendor relationships with external

[8] 14 CFR Part 101, Subpart E, is the FAA regulation that governs drone operations solely for recreation or hobby purposes.

[9] FedRAMP is a governmentwide program that provides a standardize approach to security assessment, authorization, and continuous monitoring for cloud-based services.

service providers—including its third-party vendor, which processes credit and debit card information for DroneZone registrants.

FAA Has Not Effectively Ensured That DroneZone and LAANC Have Adequate Security and Privacy Controls

FAA did not effectively assess (e.g., select, test, implement, monitor, or develop a risk mitigation strategy for) DroneZone and LAANC security controls before authorizing the systems to operate. In addition, FAA's inadequate monitoring of security controls increases the risk of the systems being compromised. Furthermore, FAA's use of unauthorized cloud systems increases the likelihood of security vulnerabilities. Finally, FAA did not adequately assess privacy and security controls for protecting PII.

FAA Has Authorized DroneZone and LAANC Operations Without Conducting a Comprehensive Assessment of Security Controls Since the System's Inception

FAA authorized DroneZone and LAANC operations for fiscal year 2019 without conducting a comprehensive assessment of the two systems' specific, common, and hybrid controls (listed in table 1) or monitoring their status. FAA has also authorized DroneZone to operate despite not taking corrective actions to address several long term weaknesses, as well as over 100 system specific control deficiencies. Additionally, both systems were authorized to operate before Agency officials learned that the wrong types of security controls were selected for about 100 hybrid and common cloud service provider controls. Furthermore, the cloud provider had major security weaknesses, which—without proper mitigation—could compromise the integrity of DroneZone as well as LAANC.

Table 1. Number of DroneZone and LAANC Security Controls, Fiscal Year 2019

Control Type	# in DroneZone	# in LAANC
System Specific	85	86
Common	73	89
Hybrid	98	82
Total	**256**	**257**

Source: OIG analysis of FAA's DroneZone and LAANC security plans and related documents.

FAA's actions did not conform to NIST requirements or DOT policy. NIST[10] states that the authorizing official[11] should maintain the information system's security posture, review security status reports and critical security documents, and determine whether significant information system changes require reauthorization actions. Similarly, DOT policy[12] states that the authorizing official is responsible for information security controls, authorization, continuous monitoring, and remediation, and should base planning decisions on an assessment of risk.

However, DroneZone's security controls were not in place when FAA initially deployed the system in December 2015. According to FAA, the controls were not in place because of increased reports of unauthorized and unsafe use of small unmanned aircraft, which posed a significant safety risk to the public. As such, FAA's intent was to quickly authorize registration service. Therefore, the SSP and System Characterization Document (SCD)—which includes these controls and other key requirements for testing and implementing them—had yet to be developed. In May 2016, FAA's independent assessor[13] identified numerous weaknesses with the system's specific security controls and requirements, as well as their implementation status. For example, FAA was not performing monthly

[10] NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011.
[11] An authorizing official is a senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations.
[12] DOT Security Authorization & Continuous Monitoring Performance Guide, January 2018.
[13] A security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).

vulnerability scans (a key control) on DroneZone and LAANC operating systems as required. Without consistently running and reviewing scans on the servers, databases, web application, and application code, the information system stakeholders are unaware of critical vulnerabilities. Therefore, stakeholders are unable to take appropriate actions to remediate vulnerabilities, resulting in increased security risk to the information systems and PII stored in the systems. Moreover, failing to remediate known vulnerabilities leaves the system more exposed to attacks that could potentially degrade system performance or compromise system integrity as well as compromise the confidentiality of sensitive data. Furthermore, the DroneZone SSP had over 100 security control deficiencies (e.g., incorrect control implementation statements, control tailoring,[14] and implementation statuses). Yet, FAA is not planning to update and reassess these security control deficiencies identified in its SSP until late 2020.

Delays in remediating these weaknesses occurred in part because FAA officials approved corrective actions without ensuring they were addressed, and because some of the Agency's plans of action and milestones (POA&Ms) lacked due dates. In some cases, POA&Ms were closed but then reopened the following year with the same weaknesses. FAA also did not continuously monitor and test DroneZone's system specific security controls in fiscal year 2017. Agency officials told us that monitoring and testing did not occur because their priority was to implement LAANC. Furthermore, despite multiple requests, Agency officials did not provide any documented evidence that the official responsible for authorizing DroneZone assessed and accepted the risks associated with failing and/or missing testing of the controls in DOT's official repository for reporting security weaknesses.

Similar issues accompanied the authorization of LAANC in 2019. FAA's independent assessor could not fully assess the status of several LAANC controls because information was missing or mislabeled in the SSP and SCD. For example, 24 security controls were marked "other than satisfied," but only 9 were entered into DOT's repository as required. All 9 weaknesses are still awaiting remediation. In total, 17 security weaknesses (3 high priorities, 11 medium priorities, and 3 low priorities) have been waiting for remediation since their initial creation dates—periods ranging from 6 to 18 months. Ten weaknesses (7 medium and 3 low priorities) lack actual start dates for remediation.

These vulnerabilities are due to a number of issues including a lack of validation that the operating system components were configured in accordance with DOT

[14] Tailoring is the process by which security control baselines are modified by: (i) identifying and designating common controls, (ii) applying scoping considerations on the applicability and implementation of baseline controls, (iii) selecting compensating security controls; (iv) assigning specific values to organizational-defined security control parameters, (v) supplementing baselines with additional security controls or control enhancements, and (vi) providing additional specification information for control implementation.

approved security configuration checklists, as compliance scans were not provided at the time of the assessment. Despite a number of requests, FAA did not provide any documented evidence that the FAA official responsible for authorizing LAANC had assessed and accepted the risks associated with not implementing the controls before authorization.

FAA's actions to authorize these systems without properly assessing controls occurred in part because FAA security officials did not have an understanding of their oversight roles and responsibilities for DroneZone or LAANC. In several meetings with OIG, DroneZone and LAANC system owners were not prepared to answer questions about how the security controls were selected, monitored, and implemented, or the inherent risks associated with those controls.

When we inquired as to who was responsible for selecting and monitoring controls, Agency officials had different answers:

- FAA security officials stated their contractor was responsible for selecting and monitoring security controls.
- The contractor program manager said that, as a contractor, it does not select security controls.
- The contractor security official expressed a need to seek clarification from FAA on how to implement security controls for the cloud service provider.
- A UAS program manager said that the Agency considers DroneZone and LAANC systems owners to be FAA business owners who do not select security controls. According to this individual, FAA relies on IT security officials to monitor the controls.
- FAA's Acting Branch Manager for Information Security and Privacy Services said the system owners work with officials in FAA's Program Management Office (PMO) to select and tailor security controls. However, a PMO official told us the PMO was not involved in selecting and tailoring controls.
- FAA security officials gave us the cloud service provider's Security Assessment Report but later acknowledged that it did not support the DroneZone security controls.
- FAA security officials and the DOT Chief Privacy Officer provided conflicting reasons to explain why the Agency did not implement privacy controls for DroneZone and LAANC.

Agency officials who do not understand their oversight roles and responsibilities are not equipped to manage the security of the DroneZone and LAANC systems and assess their security status in terms of impact, vulnerabilities, and risk. In

addition, they cannot ensure that the security controls have been properly implemented and deployed, and are operating in accordance with DOT and NIST security requirements. Finally, as the independent assessor noted, inadequate documentation can lead to misunderstandings of the system, which can result in improper functionality, delay in system recovery, inadequate resources, improper system configuration, and loss of data.

FAA's Inadequate Monitoring of Inherited Security Controls Poses a Significant Risk of the Systems Being Compromised

FAA security officials stated they do not monitor the status of the common and hybrid controls that DroneZone and LAANC inherit from the cloud service provider's public cloud computing environment. FAA and contractor representatives told us that they do not monitor these controls because FedRAMP has approved the cloud service provider. Additionally, FAA is not adequately monitoring controls it inherits within the Agency.

To help monitor inherited cloud controls, FedRAMP[15] provides the *Control Implementation Summary*, which lists the controls that cloud providers are expected to implement and those that are the customer's responsibility. Agencies can also review cloud providers' monthly continuous monitoring reports, which include reviews of vulnerability scan data, as well as updates to POA&Ms.

FAA security officials' decision not to monitor cloud service provider-inherited controls per FedRAMP guidance poses significant risks to the cybersecurity posture of both systems. For example:

- Based on our review of the cloud service provider's October 2019 POA&Ms report, DroneZone and LAANC could be subject to a major compromise of their systems because the cloud service infrastructure has key vulnerabilities. Additionally, the cloud service provider does not perform security updates (patches) or run malicious code[16] protection software on all of its operating systems. Yet, malicious code protection is one of eight system vulnerabilities that the cloud service provider has designated as operationally required.[17] Furthermore, while each system

[15] Agency Guide for FedRAMP Authorizations, version 2.0, December 2017.
[16] Malicious code is software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. An example of malicious code is a virus.
[17] A finding that cannot be remediated, often because the system will not function as intended.

inherits as many as 90 security controls from the cloud service provider, the provider does not enforce strong password requirements or implement security practices to improve the integrity and authenticity of information transmitted online. Without such protection, DroneZone and LAANC could be susceptible to a virus or another outside threat.

- FAA's authorizing officials made risk-based decisions to authorize DroneZone and LAANC operations in fiscal year 2019 before learning that there were design errors in about 100 cloud service provider security controls. For example, when we compared the DroneZone and LAANC System Security Plan Workbooks to FedRAMP's *Control Implementation Summary* for the cloud service provider's public cloud, we found that a contractor security official had selected the wrong control type for 20 DroneZone and 79 LAANC security controls inherited from the cloud service provider. This error resulted in uncertainty regarding who (the cloud service provider or FAA) was solely or jointly responsible for testing the controls and determining whether they were properly implemented or not. The contractor and FAA security officials acknowledged the controls had the wrong control type and stated that they will make corrections during both systems' fiscal year 2020 assessment.

- DOT policy[18] states that system owners can document the implementation status of systems with inherited controls in the SSP. However, we found several common and hybrid controls that had not been tested by their FAA providers—FAA Telecommunication Infrastructure and Office of Information and Technology Network. Their status was not properly documented in the DroneZone and LAANC SSP, because the controls were marked "satisfied" by FAA officials. However, FAA has not tested a major common control provider's security controls since 2015. This poses a major risk because DroneZone and LAANC rely on this provider to transport secure information between users and systems.

FAA's Acting Branch Manager for Information Security and Privacy Services told us that the Agency is working on new standard operating procedures but provided no firm timeline for when they will be complete. This official further stated that the new guidance will allow DroneZone and LAANC system owners to have more visibility into the status of inherited hybrid and common controls.

[18] DOT Security Authorization and Continuous Monitoring Guide 2018, section 4.2.3.

FAA's Use of FedRAMP-Unauthorized External Information Systems To Support DroneZone and LAANC Increases Security Risks

FAA's contractor supports DroneZone and LAANC with six external information systems (i.e., Software as a Service) that are not authorized by FedRAMP. FedRAMP has established tailored authorizations for Software as a Service systems, which are expected to have shorter timeframes through consolidated documentation and tailoring of security requirements.[19] However, FAA's contractor primary system monitoring component is still in the process of obtaining FedRAMP authorization. The lack of an authorization is an open security weakness, and FAA security officials acknowledged that they did not obtain departmental approval to use the unauthorized system monitoring component.

Additionally, the contractor uses a third-party vendor for DroneZone registration payment processing. This vendor has yet to be authorized by FedRAMP, despite FAA's independent assessor recommending that FAA ensure its payment processing vendor complete its FedRAMP certification. FAA officials stated that since the payment processing function takes place outside the system, the FedRAMP requirement does not apply. However, this is not correct. By using external information systems that are not authorized by FedRAMP, as required, FAA is increasing the risk that its DroneZone and LAANC systems could be vulnerable to cyberattacks.

According to the FedRAMP marketplace, the Federal repository for all company components providing Software as a Service, the other four external information systems that FAA's contractor uses have yet to initiate FedRAMP authorization for their systems. FAA security officials informed us that they would look into whether two of the external information systems require such an authorization, and for the remaining two they indicated FedRAMP is not applicable.

Without verifying the implementation of the required security controls on the external information systems used by individuals to access the information system, FAA cannot ensure the external information systems contain the necessary security safeguards against compromising, damaging, or otherwise harming the information.

[19] FedRAMP Marketplace Designations for cloud service providers, version 1.0; June 2019.

FAA Did Not Adequately Assess Privacy and Security Controls for Protecting PII

FAA does not have the proper safeguards in place to protect PII. In accordance with NIST guidance,[20] the Department follows the Fair Information Practice Principles (FIPPs), which establish 26 privacy controls to protect PII. However, FAA security and privacy officials could not demonstrate that the Agency had assessed and implemented 24 of the 26 privacy controls in DroneZone and LAANC security control baselines. FAA security officials stated that they did not assess the controls because Federal guidance on assessing security controls has not yet been published in full.[21] However, the referenced Federal guidance states that organizations should consult their privacy officer for direction.

DOT's Chief Privacy Officer (CPO) subsequently told us that the FAA security officials were wrong when they stated the 24 privacy controls had not been assessed. According to the CPO, the CPO's office assessed the controls. The CPO acknowledged that the Agency needs to do a better job at documenting its assessment results of privacy controls and said there is a plan to have a process in place by March 2020.

Another major security vulnerability for protecting PII occurs in LAANC's interface with UAS Service Suppliers. LAANC allows DroneZone operators to receive near real-time authorizations that UAS Service Suppliers transmit on FAA's behalf. These UAS Service Suppliers must comply with a set of technical requirements called UAS Operating Rules and security requirements in the Memorandum of Agreement (MOA) that the suppliers sign with the Agency. Through its UAS Operating Rules and the MOA, FAA collaborates with the UAS Service Supplier and allows it to retrieve the specific information it needs to ensure safe flight operations. It is important for FAA to establish MOAs with UAS Service Suppliers to protect the flying public and to safeguard their PII. However, we found FAA is not currently validating that each approved UAS Service Supplier is compliant with the security requirements[22] outlined in its MOA with FAA. This increases the risk that proper safeguards will not be in place to protect users' PII information or DroneZone. According to FAA officials, they are currently negotiating a modification to the MOAs that seeks to enhance data security and transparency. However, this plan does not address the issue of FAA's lack of verification of

[20] NIST SP-800-53 revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J: April 2013.
[21] NIST SP-800 53A Assessing Security Controls for Federal Information Systems, December 2014.
[22] NIST FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, March 2006.

whether UAS Service Suppliers are complying with the security requirements in the MOAs.

FAA Contingency Planning Does Not Adequately Limit the Effects Caused by a Potential Disruption of Services

FAA selected the incorrect control type for 9 of the 23 contingency planning controls it uses to assess DroneZone's and LAANC's ability to recover from service disruptions. We also noted other weaknesses in the Agency's contingency planning efforts. Specifically, FAA did not consistently implement its ISCP program through policies, procedures, and strategies, as departmental policy requires. Additionally, FAA did not ensure that DroneZone and LAANC external service providers performed contingency plan testing or that they make sufficient use of alternate storage and backup sites.

FAA Used Incorrect Control Types for Some Contingency Planning Controls

FAA is not effectively using contingency planning controls to limit the effects of a potential disruption to the DroneZone and LAANC systems. According to NIST guidance,[23] these controls are critical to address both information system restoration and implementation of alternative mission/business processes when systems are compromised. However, our review found that FAA's contractor incorrectly assessed 9 of 23 contingency planning controls[24] that the Agency needs to correct to effectively assess DroneZone and LAANC's implementation status. These incorrect assessments occurred because the contractor security official selected the wrong control type (e.g., common, hybrid, or system-specific) for the nine controls.

Until FAA security officials correctly update, assess, and implement these contingency planning controls, they will be unable to determine DroneZone and LAANC's ability to recover during a disruption of services. For example, one key control requires the system owner to provide for the capability to recover and restore the information system to a known state after disruption, compromise, or

[23] NIST SP-800-53 revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
[24] These include CP-2(1), CP-2(8), CP-3, CP-4, CP-4(1), CP-9, CP-9(1), CP-10, and CP-10(2).

failure. As a result of mislabeling this and other controls, FAA will have an increased risk of a disruption of services.

FAA's ISCP Program Had Many Deficiencies

FAA did not update its DroneZone ISCP and testing documentation on an annual basis, as required by the Department's policies.[25] Specifically, FAA did not document its ISCP and testing activities for DroneZone in fiscal years 2017 and 2018. Furthermore, FAA is required to establish a business impact analysis for the information system, as well as business continuity plan, disaster recovery plan, and continuity of operations plans for the system's line of business.[26] DroneZone's line of business is FAA's Office of Aviation Safety (AVS). However, FAA did not provide evidence that AVS developed the required policies and procedures.

Furthermore, we determined that FAA did not ensure that the DroneZone business impact analysis was aligned with AVS's business continuity, disaster recovery, and continuity of operations plans, per DOT policy.[27] The lack of a consistently implemented ISCP program that is defined through policies and procedures increases the likelihood that FAA's contingency plan will not be effective during an emergency. We found numerous contingency plan deficiencies at the Agency, line of business, and system levels, including the interconnected system LAANC. For example, FAA does not adhere to a key contingency planning control for information system backup that would require the Agency to test backup information quarterly, or at least annually, to verify media reliability and information integrity. Finally, FAA did not effectively communicate information on the planning and performance of recovery activities to internal stakeholders and executive management to enable officials to make accurate risk-based decisions based on the identified deficiencies.

[25] Departmental Cybersecurity Compendium 1351.37 and DOT Security Authorization and Continuous Monitoring Performance Guide, March 2018.
[26] Various lines of business, staff offices, and specialized organizations report directly to the Office of Administrator.
[27] DOT Cybersecurity Compendium, Control CP-2(1) states, "Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans."

FAA Does Not Verify Whether DroneZone's External Providers Conduct ISCP Tests

FAA cannot ensure DroneZone's continuous operations in the event of a disaster or disruption of service because it is unable to determine whether its service providers conduct ISCP tests annually, as required by NIST policy.[28] Specifically, FAA could not provide us with evidence that its external service providers—cloud service provider and contractor—had performed contingency plan testing.

For example, FAA conducted a joint ISCP test—with DroneZone and LAANC—in fiscal year 2019 but did not verify and validate that the appropriate personnel, including officials from DroneZone's line of business, were present. From FAA, the system owner, the IT point of contact, and FAA team members should have attended. From the contractor, the FAA Cloud Services service delivery manager, program manager, security manager, and primary architect should have participated as well.

This lack of verified testing occurred in part because FAA has not trained DroneZone personnel on contingency planning responsibilities and activities. As a result, FAA cannot ensure that the appropriate personnel are sufficiently aware of and understand their ISCP roles and responsibilities.

FAA Does Not Make Sufficient Use of Alternate Storage and Processing Sites

FAA does not keep its procedures for backing up and storing system data offsite up to date as required by NIST policy.[29] FAA uses an existing cloud service provider service as an alternate storage site and to ensure system failover capabilities are in place through the use of cloud service provider regions and availability zones (AZ). We found that the use of one cloud service provider region and associated AZs represent a single point of failure for the DroneZone.

However, FAA does not have a secondary method to ensure the data can be backed up and transported to an alternate site when the cloud service provider

[28] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006.
[29] NIST 800-34 states, "Backup Methods and Offsite Storage System data should be backed up regularly. Policies should specify the minimum frequency and scope of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced."

region and AZs are unavailable—a key NIST requirement when there is a single point of failure.[30] The lack of required and implemented policies for backup data and storage increases the likelihood that FAA will not be able to recover lost or compromised information during recovery efforts.

Conclusion

FAA's DroneZone system is key to the Agency's efforts to safely manage and regulate small UAS in the NAS. As such, it is vital that FAA adequately secure the system, including protecting the PII for the system's more than 1.5 million registered users. As DroneZone evolves to meet mandated and regulated requirements, it is vital that the Agency apply new, or update existing, capabilities to achieve reasonable assurance that security controls are effective. Further, FAA's security officials and its contractor must have a clear understanding of their roles and responsibilities to implement controls, including contingency planning, for all systems—including cloud-based ones. Until then, FAA's DroneZone and LAANC, as well as the PII contained within, could remain vulnerable to compromise and may become unavailable in the event of a disaster or disruption of service.

Recommendations

To help FAA strengthen its management and oversight of the DroneZone and LAANC cybersecurity posture, we recommend that the Federal Aviation Administrator:

1. Perform a comprehensive assessment of DroneZone and LAANC's security controls that at a minimum provides the correct implementation status for system specific, common, and hybrid controls, and issue a new Authorization to Operate decision for DroneZone and its interconnected system LAANC.

2. Update the security assessment documents for DroneZone and LAANC to reflect the results of all security controls (e.g., common, hybrid, and

[30] NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, pg. 32: "Cloud storage services may represent a single point of failure for the applications hosted there. In such situations, the services of a second cloud provider could be used to back up data processed by the primary provider to ensure that during a prolonged disruption or serious disaster at the primary's facilities, the data remains available for immediate resumption of critical operations."

system-specific) for selection, implementation, and assessing, per DOT requirements.

3. Establish and implement controls for monitoring, updating, and remediating open security weaknesses as well as the accepted risk in DOT repository for managing security weaknesses, per the DOT Security Weakness Management Guide.

4. Implement procedures to validate that Security Officials responsible for DroneZone and LAANC are trained on NIST and DOT policy for assessing security controls, and require them to follow the guidance.

5. Develop Standard Operating Procedures for the use of common and hybrid controls to include at a minimum:

    a. System owners must review the cloud provider Control Implementation Summary report to verify and document what controls are the customer's versus the cloud provider's.

    b. System owners must review monthly cloud provider POA&Ms and develop a risk mitigation strategy or compensating controls to address any identified vulnerabilities that may impact its system cybersecurity posture.

    c. System owners must coordinate with FAA common/hybrid control providers to verify the controls' actual implementation status and document them accurately in the appropriate security document.

6. Verify and validate that all external information systems providing cloud services to DroneZone and LAANC are FedRAMP-authorized; if not, obtain a departmental waiver approving their use.

7. Develop and implement a process clearly defining how privacy controls are identified, assessed, and documented, and work with the departmental Chief Privacy Officer in developing and implementing the process.

8. Complete modification to LAANC Memorandums of Agreement with UAS Service Suppliers to enhance data security and transparency and direct the Authorizing Official to verify and validate that all UAS Service Suppliers are adhering to security requirements outlined in the Memorandum of Agreement.

9. Develop and implement a process for testing DroneZone information systems for contingency planning, to include business impact analysis,

continuity of operations plans, business continuity plans, disaster recovery plans, and Information System Contingency Planning (ISCP).

10. Develop a process to annually document FAA security officials communicating all contingency planning development, planning, and recovery activities to all stakeholders and executive management prior to authorizing officials making risk-based decisions.

11. Complete an appropriate ISCP test for DroneZone with its contractor and cloud service provider to ensure the ISCP strategies can be implemented successfully.

12. Provide and verify that the required DroneZone personnel listed in the ISCP receive annual contingency planning training.

13. Develop, test, and implement an alternative back-up solution verifying that DroneZone data can be backed-up and available to transport to alternate sites in the event the cloud service provider availability zone is unavailable.

Agency Comments and OIG Response

We provided FAA with our draft report on March 5, 2020, and received its formal response on April 1, 2020, which is included as an appendix to this report. FAA concurred with all 13 recommendations and provided appropriate actions and completion dates. Accordingly, we consider all recommendations resolved but open pending completion of the planned actions.

Actions Required

We consider recommendations 1 through 13 resolved but open pending completion of planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between April 2019 and March 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.

Generally accepted Government auditing standards also require us to disclose impairments of independence or any appearance thereof. As part of our methodology, we assessed FAA's use of reasonable internal controls, including applicable policies and guidance on security assessment, authorization, and continuous monitoring information systems and cloud-based services issued by the FAA, its contractors, and DOT, against the NIST and FedRAMP policies. We reviewed security authorization packages for DroneZone and LAANC, which included but are not limited to: security assessment report, SSP, SSP Workbook, system categorization document, POA&Ms, and ISCP.

We interviewed security and privacy officials at FAA, DOT, and FAA's contractor support to determine the roles, responsibilities, implementation of controls, policies, and procedures for assessing DroneZone's and LAANC's security and privacy controls. We reviewed privacy-related documentation to determine whether FAA has in place all privacy controls responsible for protecting PII, and they are working as intended. Lastly, we analyzed contingency plan documentation in order to determine whether FAA has performed sufficient/adequate test activities to assess disaster recovery capabilities for DroneZone and LAANC.

We conducted our work at DOT Headquarters and FAA Headquarters in Washington, DC; and we conducted an external site visit at the contractor's location in Shreveport, LA.

Exhibit B. Organizations Visited or Contacted

FAA Facilities

FAA Headquarters, Washington, DC

FAA Air Traffic Organization (ATO)

FAA Office of Aviation Safety (AVS)

FAA Office of Finance and Management (AFN)

FAA Office of Audit and Evaluation (AAE)

FAA Office of Information and Technology (AIT)

Other Organizations

Office of the Secretary, Department of Transportation

Contractor support, Shreveport, LA

Exhibit C. List of Acronyms

AVS	FAA Office of Aviation Safety
AZ	Availability Zone
CPO	Chief Privacy Officer
DOT	Department of Transportation
FAA	Federal Aviation Administration
FedRAMP	Federal Risk and Authorization Management Program
FIPPs	Fair Information Practice Principles
ISCP	Information system Contingency Plan
LAANC	Low Attitude Authorization and Notification Capability
MOA	Memorandum of Agreement
NAS	National Airspace System
NIST	National Institute of Standards and Technology
PII	Personally identifiable information
PMO	Program Management Office
POA&M	Plan of Action and Milestones
SAR	Security Assessment Report
SCD	System Categorization Document
SSP	System Security Plan
sUASRS	Small Unmanned aircraft Registration Service
UAS	Unmanned Aircraft System

Exhibit D. Major Contributors to This Report

KEVIN **DORSEY**	PROGRAM DIRECTOR
STACY **JORDAN**	PROJECT MANAGER
JO'SHENA **JAMISON**	SENIOR IT SPECIALIST
MARTHA **MORROBEL**	SENIOR IT SPECIALIST
NELSON **FLORES**	IT SPECIALIST
AUDRE **AZUOLAS**	SENIOR TECHNICAL WRITER
SETH **KAUFMAN**	DEPUTY CHIEF COUNSEL

Federal Aviation Administration

Memorandum

Date: April 1, 2020

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: FAA Lacks Sufficient Security Controls and Contingency Planning for Its DroneZone System

The confidentiality, integrity, availability of information, and security of the information technology systems used to deliver, store, and process data are all critical to the successful operation of the DroneZone system. When the Unmanned Aircraft Systems (UAS) boom began in 2015, the FAA needed to work as quickly as possible to accommodate a new, low-risk airspace entrant that numbered in the hundreds of thousands with a system that could handle the massive quantity of information, while providing the appropriate, equivalent level of safety.

The agency expedited the implementation of a series of interim solutions. In the first week of the UAS registration service release, more than 100,000 people registered, and the FAA saw the need for an enterprise solution to consolidate and improve the processing of registrations, waiver applications, and incident reports with a new cloud-based system – the FAA DroneZone. The system provides capabilities for operators to register their drones, apply for airspace or operational waivers, check the status of their applications, and submit unmanned aircraft accident reports. There are now about 1.4 million unmanned aircraft registrations, and almost 20,000 airspace waivers and authorizations.

Additionally, FAA's automated Low Altitude Authorization and Notification Capability (LAANC) system began as a prototype in 2017. It is a collaboration between the FAA and the UAS industry that directly supports the safe integration of UAS into the nation's airspace. The system expedites authorizations to fly under 400 feet in controlled airspace. Currently, LAANC covers 300 Air Traffic Control facilities serving 500 airports, and it provides UAS operators with near-instant approval. LAANC has auto-approved over 110,000 airspace authorizations.

Upon review of the draft report, we concur with the 13 recommendations, as written, and plan to implement by the following dates:

- Recommendation 8 by May 29, 2020;
- Recommendations 1, 2, 6, 7, 9, 10, 11, 12, and 13 by September 30, 2020; and
- Recommendations 3, 4, and 5 by January 29, 2021.

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