Flight Test and Technical Evaluation Report

DJI Unmanned Aircraft System (UAS)
Mission Functionality and Data Management Assurance Assessment

U.S. Department of the Interior
Office of Aviation Services
Boise, Idaho

by

Mark L Bathrick
Brad Koeckeritz

July 2, 2019

This Flight Test and Technical Evaluation Report presents results of an assessment of the flight, payload, and data management assurance performance of the SZ DJI Technology Co., Ltd. Matrice 600 Pro and Mavic Pro unmanned aircraft systems (UAS) modified with DJI Government Edition (GE) hardware, firmware, and software for suitability in selected Interior bureau missions. Test articles were operated under the Office of Aviation Services (OAS) Test Plan for Validation and Verification of Data Security Software for Employment of DJI UAS Platforms, originally signed on April 9, 2018 and later updated with approved Modifications One and Two of November 14 and 16, 2018, respectively.

APPROVED FOR RELEASE:
MARK BATHRICK
Digitally signed by MARK BATHRICK
Date: 2019.07.08 11:11:38 -06'00'
Mark L Bathrick, Director

SUMMARY

In 2014, following four years of unmanned aircraft systems (UAS) operational test and evaluation (OT&E), the U.S. Department of the Interior's (DOI) Office of Aviation Services (OAS) and over 300 subject matter experts from DOI bureaus developed the Master UAS Requirements for the DOI. In 2015, while conducting UAS market research, OAS determined the privacy policy of the largest provider of UAS in the U.S. (SZ DJI Technology Co., Ltd) did not meet UAS data management assurance standards contained in the Master UAS Requirements for the DOI. Specifically, they did not meet DOI's requirement to be able *"to decline and lock out any device information sharing including telemetry through aircraft, software or applications preventing any automated uploads or downloads."* In 2016, Interior awarded its first contract for fleet small UAS to a U.S. based company whose aircraft met all relevant technical and DOI bureau price requirements. Shortly thereafter, the company (3D Robotics) ceased manufacturing of UAS as a result of market competition. Subsequent OAS market research to identify additional UAS to meet Interior bureaus' growing demand for inexpensive and highly capable aircraft indicated the remaining UAS available from U.S. based companies were up to 10X less capable for the same price, or up to 10X more costly than similarly capable DJI aircraft. OAS immediately began working with Interior and federal partners and the drone industry to identify, develop, and field potential solutions that met Interior's three data management and risk mitigation requirements listed in the Master UAS Requirements for the DOI. In 2017, working with the Department of Defense (DOD), OAS identified a potential solution and began developing a flight test plan to assess the suitability of this solution across a range of DOI bureau UAS missions. In 2017, OAS was also approached by DJI with an offer to collaborate on the development, testing and potential fielding of a customer-focused enterprise solution that would meet Interior's UAS data management and risk mitigation requirements for enterprise level managed data sharing controls. Draft specifications for the new "Private Edition" (later referred to as "Government Edition" - GE) included custom software, firmware, and UAS hardware editions for two specific Interior selected DJI drones (Matrice 600 Pro, Mavic Pro). Provisions to include flight testing of GE equipped DJI aircraft were later added to the flight test plan. Additionally, OAS collaborated with one industry and two federal partners with expertise in data management assurance testing to conduct targeted assessments of GE hardware, firmware, and software. While the DOD solution was secure, it provided insufficient mission functionality for DOI bureaus' complex photogrammetry, mapping, etc. mission data requirements. Flight testing of earlier versions of GE identified functional issues that were remedied in later versions. Partner led data management assurance tests of each GE version met required security exit criteria. It is recommended GE (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5) equipped Matrice 600 Pro and Mavic Pro aircraft be authorized for Interior fleet and contract use in accordance with additional risk mitigation practices developed by OAS (Appendices A, B). While the tested GE version met Interior requirements, the necessity to test and validate future GE updates to ensure continued security makes this solution time-consuming and costly to maintain and scale; not a suitable long term solution. Continued collaboration with federal and industry partners to identify additional solutions that meet DOI data management assurance requirements and are easier and less costly to sustain and scale is also recommended.

TABLE OF CONTENTS

Note: For readers viewing this report electronically, embedded hyperlinks found throughout the report provide access to additional background and reference information.

INTRODUCTION

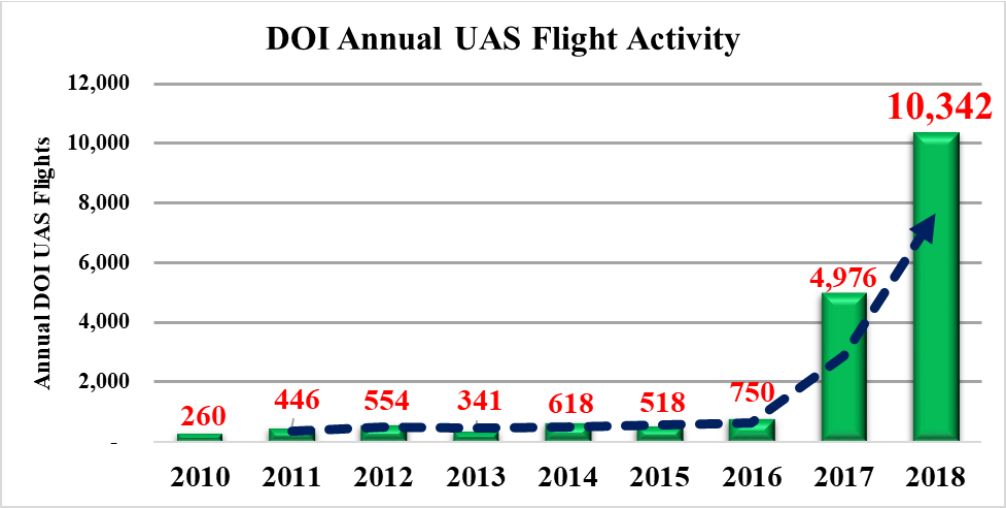
BACKGROUND

The U.S. Department of the Interior (DOI) is the largest land steward in the United States, responsible for management of 500M acres (~1 in 5) across the U.S and its territories and 1.7B acres on the Outer Continental Shelf. DOI manages resources that supply 30 percent of the Nation's energy supplies, manages water in 17 Western States and supplies 15 percent of the Nation's hydropower energy. The *"people's land,"* which DOI manages on behalf of the American Taxpayer annually hosts more than 450M visits annually.

In carrying out its extensive responsibilities on behalf of the American Public, DOI utilizes a wide variety of aircraft, including unmanned aircraft systems (UAS, aka drones). DOI missions, often conducted in remote areas, severe terrain, and weather conditions can be hazardous to personnel. These missions often require persistent presence and responsive deployment to address emergent events (e.g. wildfires, earthquakes, volcanos, floods, animal migrations, search and rescues, etc.). Mission goals include conducting them with no/minimal disturbance to native species and visitors to the lands that DOI stewards, while making the best use of appropriated funds to fulfill its chartered obligations for managing the *"people's land."* Since the initiation of DOI's current UAS program in 2006, the Department has realized significant benefits from the safe and responsible integration of drone technology.

DOI is a recognized leader in the non-military government use of unmanned aircraft systems for a variety of missions with over 600 available drones and 400 FAA certified and DOI trained operators distributed across 42 states and territories assigned to seven of Interior's nine bureaus. Since 2010 when Interior began employing UAS in operational missions, the Department has successfully flown over 19,000 UAS flights, with zero public complaints. In 2018, the DOI UAS program continued its tradition of innovation, collaboration, and leadership in the drone space. Adoption and integration of UAS in missions by DOI's nine bureaus continued to grow with **10,342** UAS flights conducted across more than 25 mission applications in 42 States and U.S. Territories in 2018; a **108% increase** in DOI UAS flights over 2017's record setting year. This included 86 flights and 382 flight hours flown in six states, supporting 16 wildfires, by commercial companies on DOI's first UAS services call-when-needed contract.

Figure 1 – DOI Annual UAS Flight Activity



Interior is also recognized as the government leader in cost-effective development and management of its unmanned aircraft systems program. Notable accomplishments in this area include:

1. Interior's Office of Aviation Services (OAS) developed and oversees Interior's award-winning UAS program with **no additional personnel or funding**.
2. All DOI's approximately 400 FAA certified and DOI trained UAS operators came from current employees; **no new hires**.
3. DOI leveraged approximately $25M in excess Department of Defense small UAS during a four year operational test and evaluation (OT&E) program that was used to inform the development of DOI's Master UAS Requirements document. Interior is the only federal agency with published UAS requirements available online to the public.
4. DOI's entire fleet of >600 fleet UAS cost less than several of the single aircraft in Interior's 93 aircraft manned fleet, averaging about $3,600 per UAS.
5. In 2018, DOI UAS use on 543 unique projects saved an estimated $14.8M over the cost of traditional ground based methods of accomplishing these projects.

Finally, Interior is also a recognized leader in UAS program transparency, privacy, and data security. The Interior Office of Aviation Services public UAS webpages contain over 200 separate technical reports, presentations, policy documents, press releases, images, videos, and news articles, which are constantly updated. Interior was one of the first federal agencies to develop and publish a Privacy Impact Assessment (PIA) specifically for UAS operations and is the only known federal agency to have published a detailed UAS Master Requirements document that includes targeted requirements intended to minimize data security risks.

UAS Data Management and Risk Mitigation

For most UAS applications, acquired data and the products derived from it (which enable better, more agile, and transparent action) are central to mission success. Effective management of UAS acquired data and mitigation of the risks of unintended distribution is a characteristic of a professional UAS program. Public experience with significant government and private sector data breaches and privacy concerns related to drones reinforce the importance of having a data management and risk mitigation strategy for all UAS programs. Although DOI has longstanding policy and procedures for the management of collected data within traditional IT systems and mission methods, UAS present additional, non-traditional challenges and vulnerabilities.

Unlike manned aircraft, most UAS and their sensors are controlled through active links with a ground control station (GCS). If the vehicle and/or sensor control link is overtaken by an unauthorized operator and the drone is flown outside the intended area of operations (or the sensor is slewed to where it should not be pointed), significant security, safety, or privacy incidents could result.

Likewise, unlike manned aircraft, most UAS actively transmit data from the vehicle/payload system to the GCS. If the payload data link is intercepted by unauthorized parties similarly significant security, safety, or privacy incidents could result which could cause embarrassment or damage to the operating organization.

Lastly, unlike manned aircraft conducting similar missions, some UAS automatically collect flight and payload data, which is often shared with the manufacturer through flight control and/or data acquisition/processing applications that connect to the internet through the GCS or other means. UAS programs unaware of whether their data is being collected, where it is going and for what purposes it is being used also risk exposure to security and privacy incidents.

DOI's UAS Data Management and Risk Mitigation Strategy

Interior's UAS data management and risk mitigation strategy is founded, like the rest of its program in solid, mission-focused requirements determination and disciplined adherence. From 2010-2014, OAS leveraged a diverse array of excess DOD small UAS (valued at $25M, but acquired at no cost) to conduct hundreds of operational test and evaluation (OT&E) flights across dozens of Interior mission applications. Based on experience and data collected during this OT&E program, over 300 Interior bureau and OAS subject matter experts came together to develop a series of Master UAS Requirements that continue to guide Interior fleet and contract UAS acquisitions (Block 1 on Figure 10).

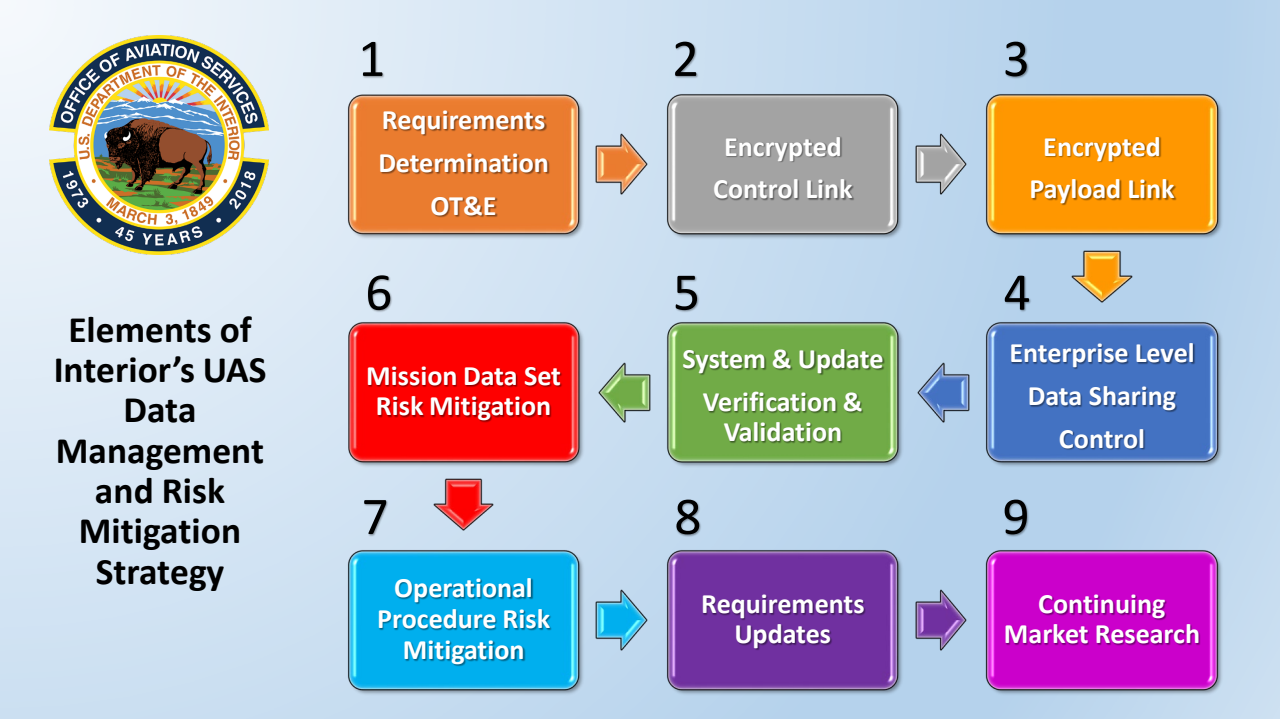
Common across the Interior Master UAS Requirements for various small UAS were three data management and risk mitigation requirements: **encrypted control link**, **encrypted payload link**, and **enterprise level data sharing control** (Blocks 2, 3, and 4 on Figure 10). Subsequent market research conducted by Interior indicated that outside the military UAS market, there were few consumer/professional UAS that met all three of these requirements. Unfortunately, tested military UAS did not meet other critical Interior mission requirements (e.g. sensor resolution, versatility, complex mapping product development) and were cost prohibitive for Interior bureaus' available funding levels,

costing up to 10X the price of similarly capable consumer models. Interior identified and acquired an initial inventory of UAS from a U.S. based company (3DR) that met the three data management and risk mitigation requirements for two UAS identified in the Master UAS Requirements for the DOI. However, shortly after this acquisition, the company was ceased UAS hardware production as a result of market pressure from other competitors like DJI.

Interior's UAS data management and risk mitigation strategy includes a commitment to verify that updates to existing Interior UAS continue to meet data management assurance requirements (Block 5 on Figure 10).

Interior's UAS data management and risk mitigation strategy also includes "non-material" measures. This includes developing mission data sets such as (a) publicly releasable, (b) sensitive, and (c) law enforcement/security sensitive data. UAS equipped with commercial UAS software from companies outside the U.S. are currently only being employed on DOI missions that collect publicly releasable data (Block 6 on Figure 10). Interior's strategy also includes employment of a system of operational training and procedural risk mitigation measures that ensures certified DOI UAS operators Interior are trained in their use and follow strict protocols designed to support the embedded enterprise data management functionality (Block 7 on Figure 10). Lastly, Interior strategy includes continual updates to its UAS requirements based on mission experience and to collaborate with industry to ensure mutual understanding of current and emerging requirements and technology (Blocks 8 and 9 on Figure 10).

Figure 2 - Elements of Interior's UAS Data Management and Risk Mitigation Strategy.



The size of the DOI UAS fleet and bureau demands for providing more current employees with UAS training has grown extensively over the last few years in direct response to the growing adoption of this technology by our Interior bureaus and the measured improvements in ***Sensing, Safety, Savings,*** and ***Service*** UAS have brought to DOI. This growth is due to the ability to utilize inexpensive small UAS that performed very well in support of the Bureau missions.

Figure 3 -

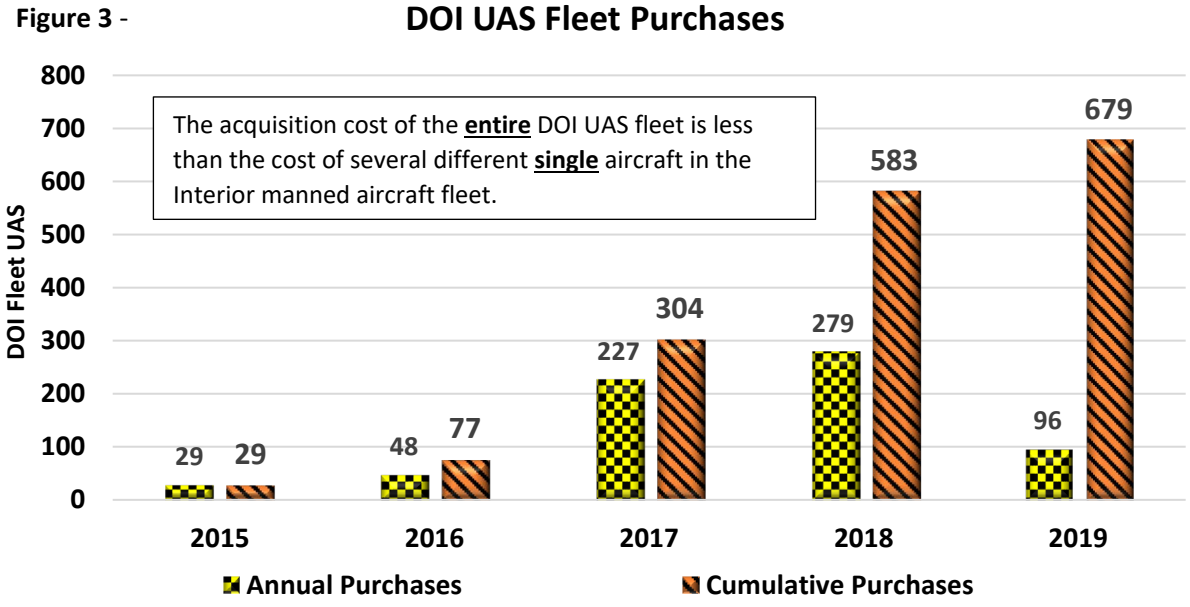
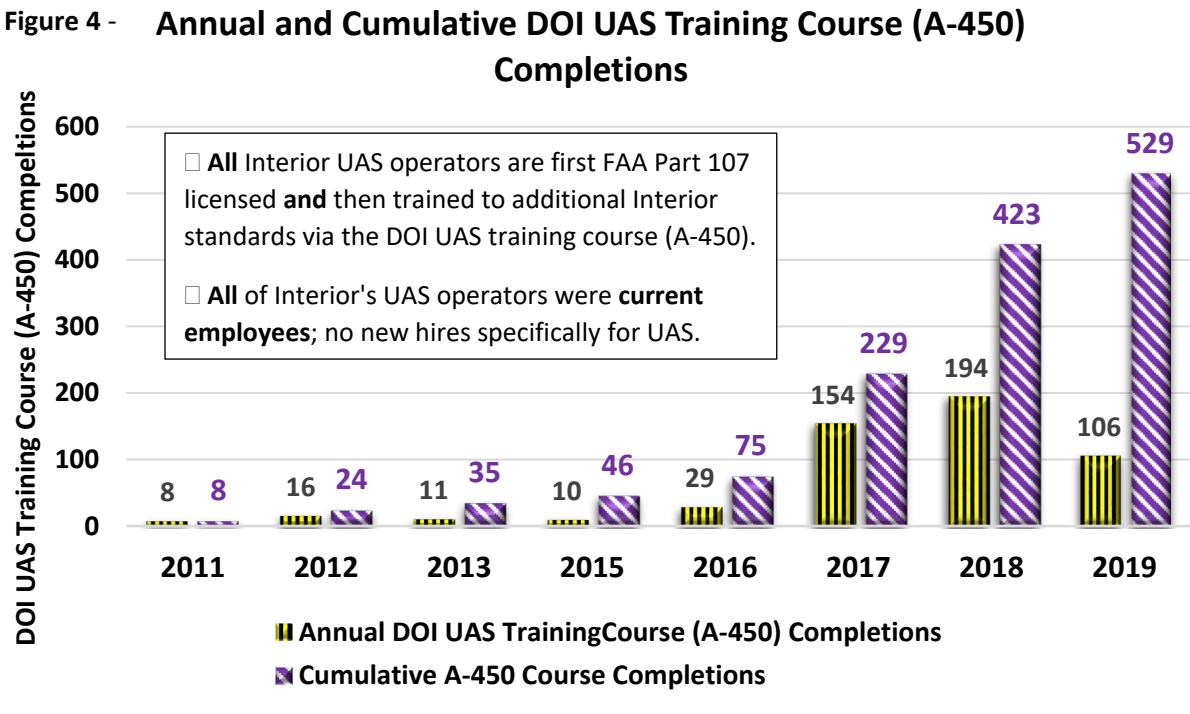


Figure 4 -



The U.S. based company (3D Robotics) that produced the commercial UAS first acquired by and most widely used by DOI is no longer in making aircraft due to market competition. DJI, a Chinese based company currently has the vast majority of the market share for small UAS. Their aircraft perform well and are available at a price point that make them attractive to the constrained budgets of Interior bureaus. However, there are known security vulnerabilities with off-the-shelf DJI equipment that preclude DOI's use of DJI equipment. DOI has been working with DJI for over two years to create a solution that would allow the bureaus access to high quality DJI hardware while at the same time preventing unwanted data leakage to any outside entities. This report details actions taken by OAS to facilitate access to low cost/high quality UAS for the bureaus while still maintaining the integrity of DOI data collected by these aircraft. OAS has done exhaustive market research and has been unable to locate a domestically available product that is competitive from a price or performance standpoint.

PURPOSE

The purpose of this evaluation was to examine the validation, verification, and utility of custom software, Firmware and applications in solving known cyber security issues with DJI products. The intent of creating these solutions was to facilitate employment of these low cost aircraft across the full range of DOI missions. OAS served as the lead flight test agency under its Departmental Manual (DM) authority to ***"conduct DOI aircraft and equipment research and development efforts"*** as defined in 350 DM 1 and its responsibility for ensuring the Secretary's and Department's legal and regulatory requirements as defined in 49 U.S.C. § 40102(a)(41), FAA Advisory Circular 00-1.1B, and Federal Management Regulations (FMR 102-33) for Public Aircraft Operations (PAO) are met.

TEST EQUIPMENT - HARDWARE, FIRMWARE, SOFTWARE AND APPLICATIONS

The equipment for the test program included:

Hardware

- 20 DJI Matrice 600 Pro (M600P) Hexacopters
- 41 DJI Mavic Pro Quadcopters
- Apple IPads
- Android Tablets
- Proprietary DJI Cameras
- COTS cameras
- Custom USGS Gas Sensors
- Livestreaming Equipment
- Ignis Payload

Firmware

- DJI Government Edition custom firmware

Software

- DJI Government Edition Assistant 2 software
- DOD provided custom software – separate tests

Applications

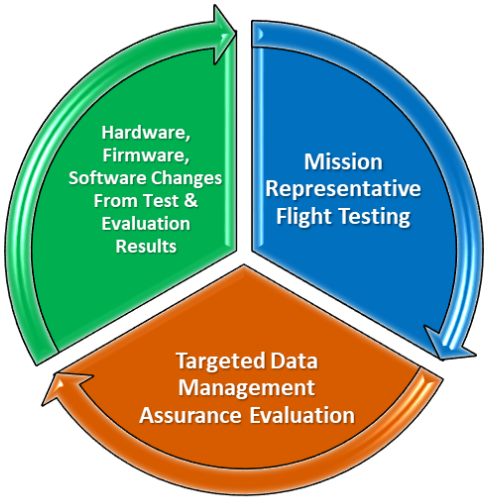
- DJI Government Edition Pilot App for Android
- DJI Government Edition GSPRO for IOS.

The two test aircraft models (M600 Pro and Mavic Pro) were chosen based upon the highest bureau priorities among the remaining unmet requirements in the Master UAS Requirements for DOI.

SCOPE OF TESTS

The scope of this testing program included conducting trials of the custom software/firmware and applications as well and verification that the solution prevents unwanted data leakage. Testing of the hardware/software for operating the M600 Pro and the Mavic Pro began in April of 2018 as part of the three phase testing plan developed by OAS. **Since the beginning of testing, there have been 1,133 flights totaling 298 hours on the M600 Pro and 1,112 flights totaling 240 hours for the Mavic Pro**. Much of the testing occurred during operational missions. A variety of payloads were tested including; electro-optical (EO) and Infrared (IR) cameras, gas detection sensors and an aerial ignition payload. Testing of the aircraft was limited to a limited number of qualified pilots for completing the test plan. In addition to the flight testing OAS collaborated with a private contractor, the National Aeronautics and Space Administration (NASA) Kennedy Space Center and another federal agency and national laboratory to complete a cybersecurity assessment of the custom hardware/firmware package. All reports independently came to the same conclusion. In their testing there was no indication that data was being transmitted outside the system and that they were operating as promised by DJI. DOI has ongoing collaboration with other governmental organizations to validate its security solutions. In addition to the DJI provided GE software, OAS also conducted functional flight and mission assessments on DOD provided software. Specific results of the DOD tests were shared with DOD, but were "For Official Use Only" and are not covered in detail in this report.

Figure 5 – Project Approach



TEST OBJECTIVES

The objectives of Phase One and Two of the DOI data management test plan was to validate whether the cyber security solutions provided to DOI from DOD were suitable for larger distribution across DOI. This included both an assessment of the functionality of the aircraft along with the quality and utility of the sensor data collected by the test aircraft. The objectives of Phase Three were to validate the efficacy of GE in a wide range of bureau missions in representative field environments and conditions. Objectives of specific cyber assessments led by applicable industry and federal partners were to validate the data management assurance claims of GE on the two DJI platforms of interest.

TEST PHASES AND EXIT CRITERIA STANDARDS

FUNCTIONAL AND MISSION FLIGHT TESTING PHASES

PHASE One (OAS testing) **COMPLETED**

Test Tasks – Obtain needed hardware and software for initial testing.

- Acquire M600 Pro platform.
- Acquire Mavic Pro platform.
- Receive custom software firmware and applications from DJI.

Required Exit Criteria - MET

- Apps validated sufficient from a security standpoint – no data transfer.
- Apps connect to the UAS as advertised.
- Functionality of the apps is as expected.

Phase Two (OAS Operational Testing) **COMPLETED**

Test Tasks:

● Field-testing of full functionality of the aircraft using secure GCS software (minimum of 12 takeoffs and landings).

- Arming
- Takeoff
- Climbs
- Turns
- Range
- Endurance
- Speed
- Comm Link
- Emergency Procedures
- RTL
- Manual Landings
- Auto landings

- Field-testing of Ignis aerial ignition payload on M600. Install and bench test payload.
- Drop inert spheres for three cycles to ensure no anomalies.
- Drop live spheres to ensure full function of the payload. ▪ Goal is 2500 spheres but is subject to weather constraints.
- Successful test deploy aircraft with OAS operators to conduct live burn with Bureaus. This requires purchase of second M600 for backup.

Field Testing of M600 Pro and Mavic Pro **COMPLETED**

Figure 6 *- Department of Interior remote pilots Chris Holmquist-Johnson (USGS) and Rich Thurau (OAS) prepare for M600 Pro UAS night operations near "fissure eight" on Hawaii's big island. On one such flight, a DOI UAS team used an M600 Pro to conduct a lifesaving search and rescue mission, saving a local resident from a fast moving lava outbreak.* *(Photo credit, Mark Bauer, USGS).*

- Arming
- Takeoff
- Climbs
- Turns
- Range
- Endurance
- Speed
- Comm Link
- Emergency Procedures
- RTL
- Manual Landings
- Auto landings
- Use of goggles

Figure 7 - *Department of Interior remote pilots conducting Mavic Pro UAS night lava mapping and monitoring operations near "fissure eight" on Hawaii's big island. DOI conducted more than 1,200 flights from May and September of 2018 to support tracking eruption activities. (Photo courtesy of USGS)).*

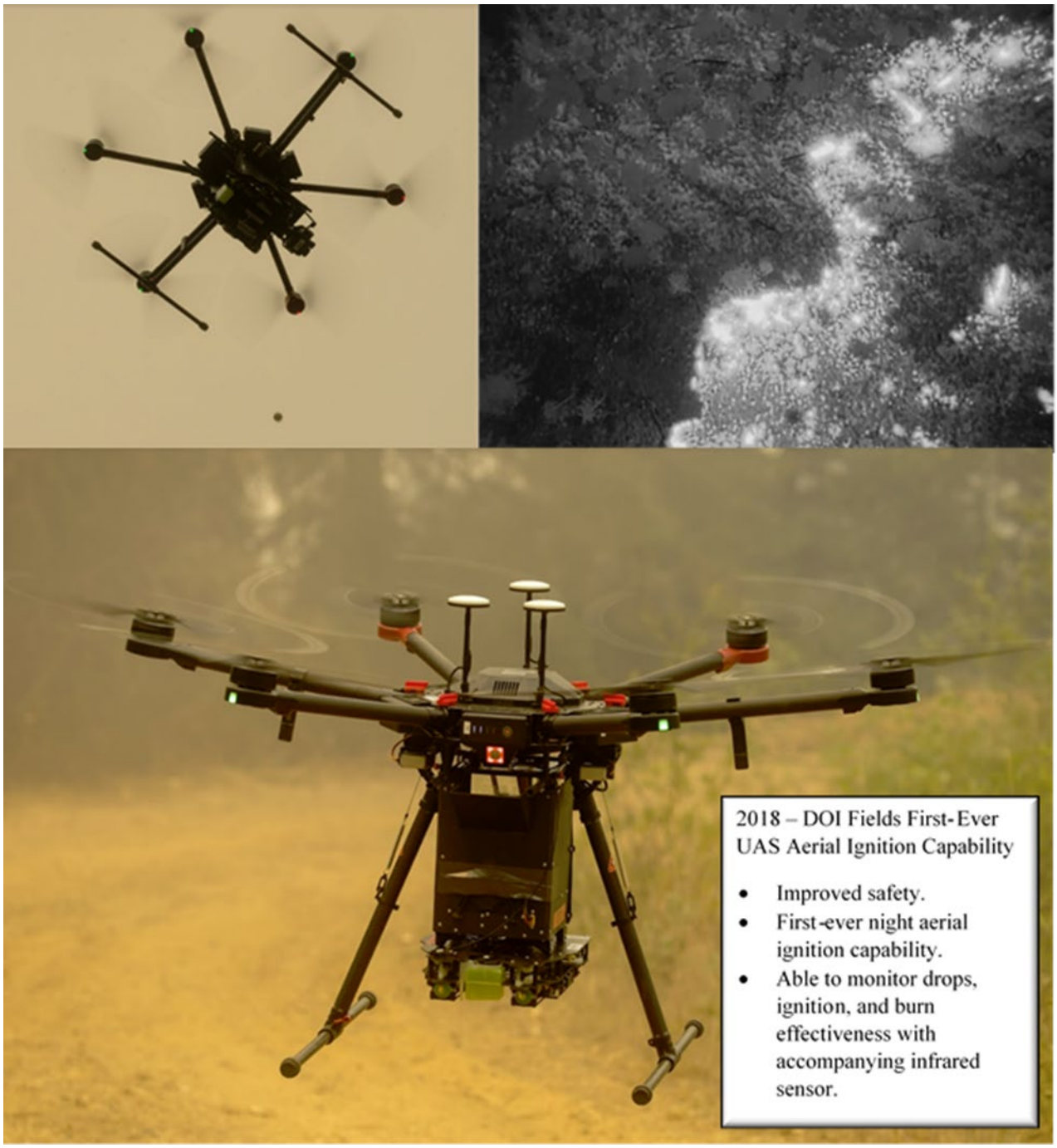


Figure 8 - *The Drones Amplified Ignis plastic sphere dispenser (PSD) provided firefighting UAS remote pilots with a new tool in 2018. The UAS-mounted PSD payload (lower center image) reduces risks to personnel who would otherwise create backing fires (viewed through the on-board infrared camera in the upper right image) by walking with a drip-torch or by flying manned helicopters in hazardous conditions. This payload was flown 177 times for more than 50 hours in fiscal year 2018. The aircraft and payload can be seen in action in the upper left image.*

Required Exit Criteria – MET

- Hardware/Software perform as expected.
- No unexplained anomalies that affect the safety of flight or performance of the aircraft.

PHASE Three (Bureau Operational Testing)

TEST TASKS: COMPLETED

- Identify with bureaus the number of M600 and Mavic Pro aircraft they would like to acquire NTE 20 M600 Pro and NTE41 Mavic Pro Aircraft.
- OAS will configure the aircraft with the secure apps and provide the bureau with the aircraft and tablet in the secure configuration.
- Bureau operator will sign an agreement that the will only operate the aircraft in the secure configuration and will make no modifications without OAS approval.
- Bureaus will deploy aircraft for mission work over a 3-month period.
- OAS will monitor usage and provide technical support to bureaus as needed.

Required Exit Criteria – MET

Agreement between OAS/Bureaus that the solutions are a viable fix and are sustainable over time.

DATA MANAGEMENT ASSURANCE TESTS AND EXIT CRITERIA

In addition to confirming the flight and mission functionality of GE equipped M600 Pro and Mavic Pro test articles, it was critical to conduct data management assurance assessment tests to validate GE claims. For these tests, OAS turned to one industry partner and two federal partners for assistance, each with demonstrated expertise in this competency.

Drones Amplified, Inc. was selected as the industry partner to assess the data management assurance of the first version of GE provided to OAS. Drones Amplified had previously provided Interior with a similar assessment of DJI's "Local Data" mode, identifying data management assurance issues which were critical to OAS's decision to not authorize the use of DJI products with Local Data mode and to continue working with DJI on a solution that would meet Interior's requirements. The purpose of this evaluation was to determine if the systems leak data to DJI servers under certain operational conditions, and to determine the degree the systems can be operated without connecting to the internet, including the use of the IGNIS payload. Additionally, they were to examine whether or not the specialized drones were prevented from connecting to the publicly-available versions of DJI software, a key Interior requirement. Drones Amplified concluded in their report that ***"the specialized software did not leak data under the investigated operational conditions."*** Drones Amplified made several recommendations for changes to that version of GE software that were incorporated by DJI in the next version. The full Drones Amplified report can be found at Appendix D.

The National Aeronautics and Space Administration (NASA) Kennedy Space Center conducted tests to capture and review all network traffic for the updated version of GE that resulted from recommendations stemming from the Drones Amplified report discussed above. NASA's conducted test to ensure Interior's concerns with data integrity with respect to the updated GE software were addressed. High level objectives of the NASA review included:

1. Data loss prevention: preventing the disclosure of NASA data to potentially hostile foreign entities.
2. Data egress control: preventing the egress of non-NASA data to superfluous and potentially hostile entities.
3. Operational functionality: Continue to provide full GE functionality while meeting objectives 1 and 2.

Interior provided NASA with the DOI version of the DJI GE software, which uploaded to DJI UAS NASA had previously procured. In order to verify the DOI version of the DJI GE software prevents NASA data from reaching potentially hostile foreign (PRC) entities, a system end-to-end test was conducted. In addition to capturing a complete network traffic snapshot of the DOI GE version of the software, a network traffic snapshot for the commercial version of the GE was also captured for comparison. The test was performed as follows:

1. iPad was wirelessly connected to internet using the described test configuration.
2. iPad was connected to aircraft controller and GE software kicked off.
3. Aircraft was powered up and linked to controller.
4. A series of GE functions were tested including downloading maps of flight location.
5. All network traffic was captured by Wireshark for analysis.

This process was repeated for both the commercial and DOI version of the DJI GE software package. NASA's test determined the DOI version of the GE software did not communicate with servers in China, and appeared to prevent the unintended disclosure of UAS data when compared to the commercial-off-the-shelf (COTS) released DJI software. As Drones Amplified did in their test and reporting on the initial version of GE, NASA made recommendations for changes to GE that were incorporated in the third version provided to OAS for flight, ground, and lab testing. NASA's report was labeled "Official Use Only" and as such is not included as an appendix to this report.

In early 2019, OAS collaborated with another federal agency and their national laboratory partner to provide a third independent assessment of the updated current version of GE. The objective was to validate data management assurance claims for this third version of GE, updated as a result of previous OAS and partner flight, ground, and lab tests. For this limited scope test and evaluation (T&E) program, OAS provided the test team with representative UAS test articles and accompanying GE software, firmware, and hardware. The limited scope analysis focused primarily on the following elements:

1. Government edition data leakage related to hardware-software interface
2. Video/Telemetry Streaming (@2.4 GHz or 5.8GHz depending on model frequency and protocol)
3. Other wireless spectrum analysis to identify signals and protocols
4. Identification of data exfiltration points
5. Initial Software/Firmware assessment on the platform and ground controller
6. Review of default configuration, certificate storage and key management
7. Initial reversing of candidate system binaries (typically encryption binaries)
8. Vulnerability mitigations measures, best practices and future areas of analysis

Test and evaluation project commitments included an initial analysis results delivery, completion of the limited scope analysis, and delivery of a final study. The project team recently concluded the initial analysis results delivery. They unanimously agreed ***"the limited scope analysis findings support the mitigations DOI has in place are in fact working as designed."*** The final report for this effort will also be "Official Use Only."

Required Exit Criteria – MET

ADDITIONAL DATA MANAGEMENT ASSURANCE RISK MITIGATION MEASURES EMPLOYED

Successful risk mitigation in any endeavor is a combination of material and non-material measures. As an example, an altitude warning system (material measure) won't keep an aircraft from crashing without thoughtful and well-executed policies and practices that serve to keep aircraft and pilots from getting into extremis altitude situations in the first place (non-material measures). In addition to working with partners to develop, test, and field UAS that meet Interior data management assurance requirements, OAS has also implemented non-material measures to further mitigate risks.

Separation from the DOI Network – From the inception of the current DOI UAS program in 2006, OAS has also coordinated with the Interior Office of the Chief Information Office (OCIO) on data management assurance. In 2008, as part of OAS's strategy to conduct a cost-effective operational test and evaluation (OT&E) of existing UAS technology to inform future Interior UAS requirements, OAS obtained nearly $25M in excess Department of Defense (DOD) small UAS. Since those aircraft came with laptops as controllers, OAS discussed it with the OCIO and agreed they wouldn't be connected to the DOI network. Later, after it was determined DOD UAS didn't fully meet Interior requirements, OAS reached out to OCIO to coordinate the introduction of commercially procured UAS into the DOI fleet. As we evolved and started purchasing both tablets and laptops we again discussed this with the OCIO. Similar to the tablets used to control the DOD UAS and the iPads present in DOI's manned aircraft fleet, OAS and the OCIO agreed to keep UAS associated control tablets and planning laptops separate from the DOI network. Additionally, OAS, OCIO, and the bureaus agreed OCIO would not provide support for UAS related IT equipment, reducing costs to our bureaus. In over 10 years of Interior UAS operations, this off-network policy has successfully prevented any related data security issues. This proven practice also serves as the foundation of one of Interior's non-material risk mitigation measures for GE. As depicted in the process flow diagram in Appendix A, , GE software is kept from connecting to the DOI network, utilizing only off-network ground control station (GCS) computers and tablets to transfer and upload GE software. Data derived from GE supported flights is physically removed from the UAS and only then via this air gap physically inserted into OCIO approved DOI computers for data downloading and processing (using only OCIO approved software).

Follow-On GE Software, Firmware, Hardware, and Application Assurance Process – Another risk mitigation measure Interior has developed is the practice of performing a spot-check validation of subsequent updates by a third-party partner before they are authorized for DOI fleet introduction. This detailed process flow diagram can be found in Appendix B.

Mission Selection Risk Mitigation – Another data management assurance risk mitigation measure is to only employ UAS on non-sensitive missions that only collect publicly releasable data.

TEST ENVELOPE

All tests were conducted with the flight envelope and operating limits of the M600 Pro and Mavic Pro, respectively. Additionally, all tests were conducted in accordance with Interior's UAS authorized UAS areas, Federal Aviation Administration (FAA) and DOI rules, policies and standards for operating UAS, and expanded operating authorities granted by the FAA through signed formal agreements.

TEST CONFIGURATIONS AND LOADING

All test configurations and loading were in accordance with OAS authorized payloads for the M600 Pro and Mavic Pro.

METHOD OF TESTS

TEST METHODS AND PROCEDURES

Test flights were all conducted in accordance with written and publicly available DOI aviation policy. Test flights were performed both in dedicated flights with specific functional assessment objectives and across a variety of Interior UAS missions including:

1. Volcano response and monitoring.
    a. Gas detection, assessment, and monitoring.
    b. Crater mapping.
    c. Lava flow speed determination.
2. Search and Rescue (SAR).
3. Prescribed fire area inspections.
4. Aerial ignition in support of wildland firefighting.
5. Wildland fire perimeter mapping.
6. Wildland fire pre/post vegetation mortality mapping.
7. Ground-penetrating radar payload assessment.
8. Emergency equipment delivery (proof of concept).
9. Volumetric determination for surface mining.
10. Water sampling.
11. Doppler radar for stream flow measurements.
12. Methane gas detection.
13. Beach sand tidal distribution volumetric mapping.
14. Light Detection and Ranging (LIDAR) assessment and application.
15. Archeologic and historical site mapping.
16. Dam infrastructure mapping and inspection.
17. Animal species population density census.
18. Avian off shore nesting site inspections.
19. Aircraft accident mapping and inspection.
20. Situational awareness and reconnaissance flights for managers with live streaming.
21. Tethered power supply testing for persistent surveillance and reconnaissance.
22. Operator training.

Quantitative data was collected and qualitative assessments were made during each project test flight.

CHRONOLOGY

1.	Current DOI UAS program initiated by OAS	2006
2.	OAS collaborates with DOD, FAA, NASA to develop DOI UAS program	2007
3.	OAS collaborates with DOD to obtain excess Raven and T-Hawk small UAS for OT&E	2008
4.	OAS and Interior bureaus conduct OT&E to inform requirements determination	2010
5.	FAA grants pilot written exam equivalency to OAS-developed UAS training curriculum	2013
6.	OT&E with excess DOD UAS completed	2014
7.	300 bureau and OAS experts use OT&E results to develop Master UAS Requirements	2014
8.	OAS market research identified data management assurance issues in DJI privacy policy	2015
9.	First DOI UAS fleet contract awarded	2016
10.	OAS begins collaboration with DOD on potential data management assurance solutions	2016
11.	OAS develops data management assurance test plan for selected DJI UAS platforms	2018
12.	Data analysis and report completed	July 2, 2019

RESULTS AND DISCUSSION

TEST RESULTS - AS RELATED TO THE OBJECTIVES AND THE MISSION

Hardware

The opportunity to utilize the test aircraft during the volcano response allowed for much more testing than originally anticipated. There were **667** Mavic Pro flights and **695** M600 Pro missions conducted during Phase Two of the test plan. Operationally the hardware performed well.

In the volcano response mission, the aircraft monitored volcanic activity, measured emitted gas types and concentrations, mapped crater collapse, measured lava flow rates, and were used to effect a lifesaving rescue. Additional details, video, and images related to test flights in the volcano response mission can be found at the following link: https://www.doi.gov/aviation/uas/doi-uas-teams-supporting-volcano-monitoring-emergency-response-rescue

In the aerial ignition mission, the aircraft were employed in firing support of daylight and first-ever nighttime burnout operations on a wildfire, using the Ignis plastic sphere dispenser (PSD) payload. Additional details, videos, information papers, field reports, and related news articles can be found at the following link: https://www.doi.gov/aviation/uas/doi-uas-aerial-ignition-aggressively-managing-fuels-enhanced-efficiency-and-safety

In tests that examined the M600 Pro in the emergency equipment delivery mission for possible search and rescue applications, the aircraft performed as desired. A presentation and embedded videos on this specific test effort can be found at the following link: https://www.doi.gov/sites/doi.gov/files/uploads/april_2018_preliminary_test_results-oas_unmanned_aircraft_systems_uas_testing-emergency_equipment_delivery.pptx

No aircraft were lost or damaged due to mechanical issues during tests. There were three mishaps with the Mavic Pro due to operator error. Two were forced landings due to battery depletion in locations where they

were not safe to retrieve. The third was due to water penetration causing loss of flight control during a rainstorm. The M600P hardware performed better than Mavic Pro, primarily due to its excess power available, which made it more capable in managing high wind conditions. There was one mishap due to operator error with the M600 resulting in minor damage that was repaired in the field.

Firmware

The provided firmware performed well and there was no outward indication that it caused any change to aircraft flight performance or handling qualities. Loading the firmware was straightforward and was relatively easy to do from a fleet management perspective. Over the course of the testing, DOI provided substantial feedback to DJI on the functionality of the aircraft. As a result of this feedback, DJI modified the firmware several times during the testing period. The goal of this development was to get the firmware/software to a stable configuration that we can scale across the department. New applications/firmware updated provided to DOI during testing were vetted through one of our review partners prior to distribution to flight testing.

Software

One of the major vulnerabilities with respect to UAS cybersecurity occurs during the update processes using PC based software. If updates are done “over the air” there is a large amount of encrypted data that flows between the user and the manufacturer. This encryption is primarily to protect the manufacturer’s intellectual property. DOI identified in 2015 that “over the air” software/firmware updates did not meet our requirements related to data management assurance. In response, DJI worked with DOI to build a custom “Government Edition” (GE) version of their Assistant 2 software. This version runs offline of the DJI servers and there are no “over the air” updates to the aircraft. GE firmware is downloaded from the manufacturer and side loaded into the aircraft using the secure version of Assistant 2, preventing data leakage during this process. The provided software performed well inflight. Data management assurance tests performed by our industry and federal partners indicated the software did not “leak” any data.

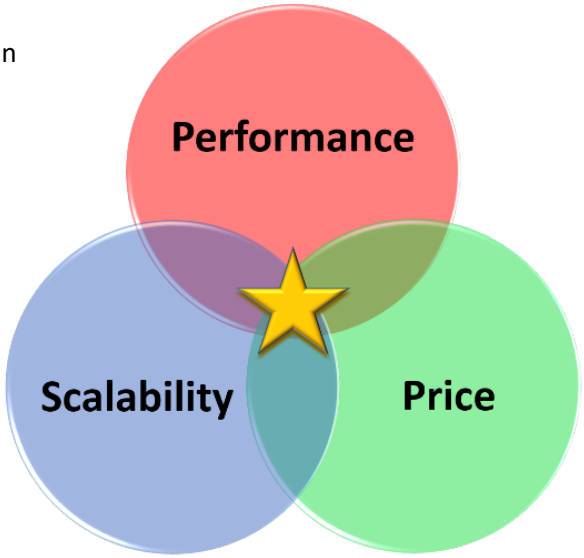
Applications

Applications used to operate UAS are an area of significant potential vulnerability. With respect to DJI, their applications are heavily integrated on the back end with DJI servers. This makes it very easy for a user to intentionally and possibly unintentionally share data with the manufacturer that organizations may not want to share. In addition to custom firmware and hardware, DJI also produced custom GE applications for DOI to address concerns with data leakage. DOI provided feedback to DJI on the functionality of each GE version of these applications. The final build of custom GE applications support both Android and IOS usage. The final version of these applications was evaluated for functionality and security. That analysis confirmed they are performed as advertised and confirmed the only "call out" from the system was to the Mapbox server located in the US. Obtaining map data is required for the purposes of flight planning.

CONCLUSIONS

1. The final tested version of the DJI Government Edition (GE) solution (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5) provided a reasonable mitigation for known data management assurance vulnerabilities of the stock Matrice 600 Pro and Mavic Pro UAS.
2. Observed test results cannot be extended to future DJI GE software, firmware, or hardware updates. To ensure continued data management assurance, subsequent GE related updates will require additional validation and verification (V&V) testing before approvals can be granted for future versions. This necessary V&V testing of future updates will result in added program costs and delays, dependent on the number and complexity of proposed changes. Accordingly, the GE solution by itself does not represent a long term, sustainable solution for Interior. Future solutions must provide consistent levels of data management assurance without the need to conduct costly and time-consuming V&V of subsequent updates.
3. Any residual unknown data management risks associated with GE could be further mitigated by employing the two tested UAS only on missions that collect non-sensitive, publicly releasable data.
4. DOI market research indicated there are currently no domestically available alternatives that are competitive in **price**, required mission and security **performance**, and necessary **scalability** to the two tested UAS.

Figure 9 – UAS Selection Considerations



RECOMMENDATIONS

1. Approve the acquisition of M600Pro and Mavic Pro aircraft in the Government Edition configuration (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5) as part of the DOI UAS fleet.
2. Maintain third party validation of any new or updated software, firmware, hardware, or ancillary DJI applications to ensure no data leakage occurs with these updates.
3. Limit approved GE equipped M600 Pro and Mavic Pro aircraft to non-sensitive missions that collect publicly releasable data.
4. Provide all DOI UAS operators and bureaus operating DOI UAS with copies of (a) DOI UAS Best Practices for Responsible Operations and (b) Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) CYBERSECURITY BEST PRACTICES FOR OPERATING COMMERCIAL UNMANNED AIRCRAFT SYSTEMS to.
5. Continue ongoing work between OAS, DOI bureaus, OCIO, industry and federal partners to identify long-term UAS data management assurance solutions that are (a) Federal Risk and Authorization Program (FedRAMP) compliant, (b) aligned with the **price** requirements of Interior bureaus' budget constraints, (c) support the breadth and complexity of DOI mission data processing **performance** needs, and (d) are easily **scalable** across the growth and future diversity of DOI's UAS fleet and supporting contractor vendors.

Figure 10 – FedRAMP Governance is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program.

ABOUT THE AUTHORS

Mark L. Bathrick – Director, Office of Aviation Services (OAS)
CAPT USN (Ret)

Mark has over 35-years' experience in aviation operations, testing, acquisition, and leadership; more than 30 in unmanned aircraft systems (UAS). Prior to his current position, Mark completed a distinguished career as a decorated Navy fighter pilot, TOPGUN graduate, experimental test pilot, chief test pilot, multiple squadron commander, and installation commander, where he received a Presidential award for leading the top base in the Navy. Mark also served in high level budget and acquisition roles in the Pentagon where he managed accounts totaling over $4.5B. As OAS Director, Mark has consistently reduced costs and increased productivity by instituting industry best practices and lasting cultural transformation. Under Mark' leadership, OAS manages 54% more aviation contracts, 540% more fleet aircraft, 395% more fleet pilots, and oversees 21% more bureau aviation units with 3% fewer people and 21% less inflation-adjusted funding than in 2007. Mark is the architect of Interior's industry leading UAS program; recognized as the largest, most diverse non-military drone program in the world, developed with no additional staff or funding. Under Mark's leadership, Interior's UAS program achieved $14.8M in net operational savings in 2018 alone. Mark received the 2017 Commercial Drone Alliance Industry Heroes, End User Innovator of the Year Award. In 2018, he was named by Commercial UAV News as one of the Top 7 Drone Visionaries in Commercial Markets. Mark holds a Bachelor of Science in Aerospace Engineering from the U.S. Naval Academy and an MBA from Boise State University. Mark is a member of the Society of Experimental Test Pilots, the National Engineering Honor Society, Tau Beta Pi, and was inducted into the University of Idaho's Academy of Engineers in 2017.

Brad Koeckeritz - Chief of the UAS Division, Office of Aviation Services

Brad began his career as wildland firefighter on the front range of Colorado in 1992. Prior to joining the Office of Aviation Services he was the crew supervisor for the Teton Interagency Helitack Crew where he spent 10 years conducting fire and search and rescue missions for the Bridger-Teton National Forest and Grand Teton National Park. Along the way he earned a B.S in forestry from Colorado State University and obtained private and commercial pilot's certificates and is a certified flight instructor (CFI, CFII, MEI). Brad began his work with UAS in 2010 when he was asked to manage the small UAS training program for DOI. In his role at OAS he oversees the UAS policy, standardization and fleet management for the U.S. Department of the Interior. He serves on several intergovernmental groups to facilitate the safe and effective integration of UAS in the national airspace.

REFERENCES

(a) U.S. Department of the Interior Office of Aviation Services Technical Report – DJI Unmanned Aircraft System (UAS) Data Management Assurance Evaluation dated July 2, 2019

(b) 49 U.S.C. § 40102(a)(41), 49 U.S.C. § 40125

(c) Federal Management Regulations (FMR 102-33)

(d) Federal Aviation Administration Management Advisory Circular 00-1.1B

(e) 112 DM 12, 350 DM 1

(f) 14 CFR PART 107—Small Unmanned Aircraft Systems

APPENDICES

Appendix A - Government Edition (GE) Off-Aircraft Data Security Risk Mitigation Processes and Protocols

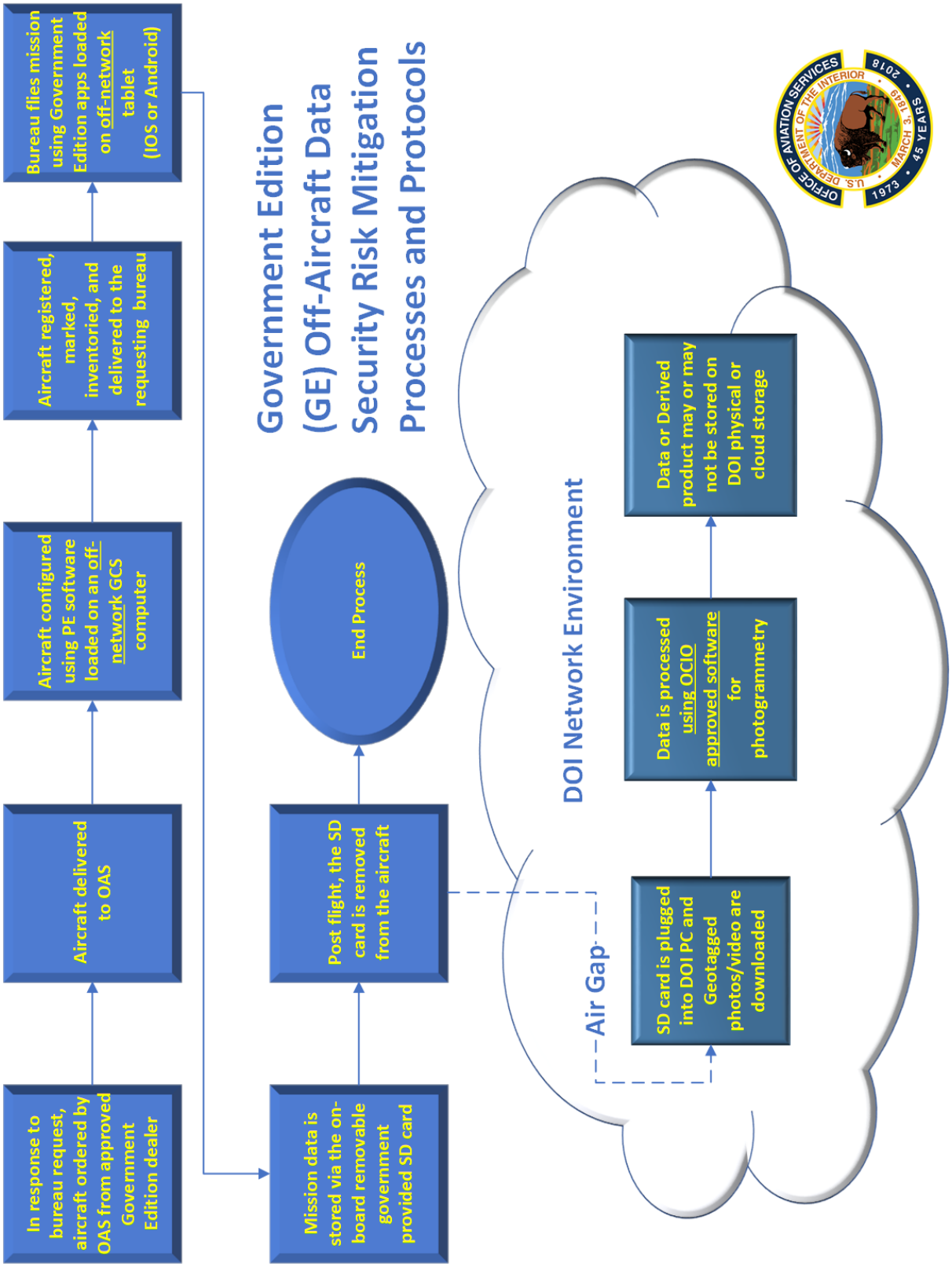
Appendix B - Process to Validate Future Government Edition (GE) DJI Software, Firmware, Hardware, and Application Updates Continue to Meet Interior Master UAS Requirements

Appendix C - Test Plan for Validation and Verification of Data Security Software for Employment of DJI UAS Platforms

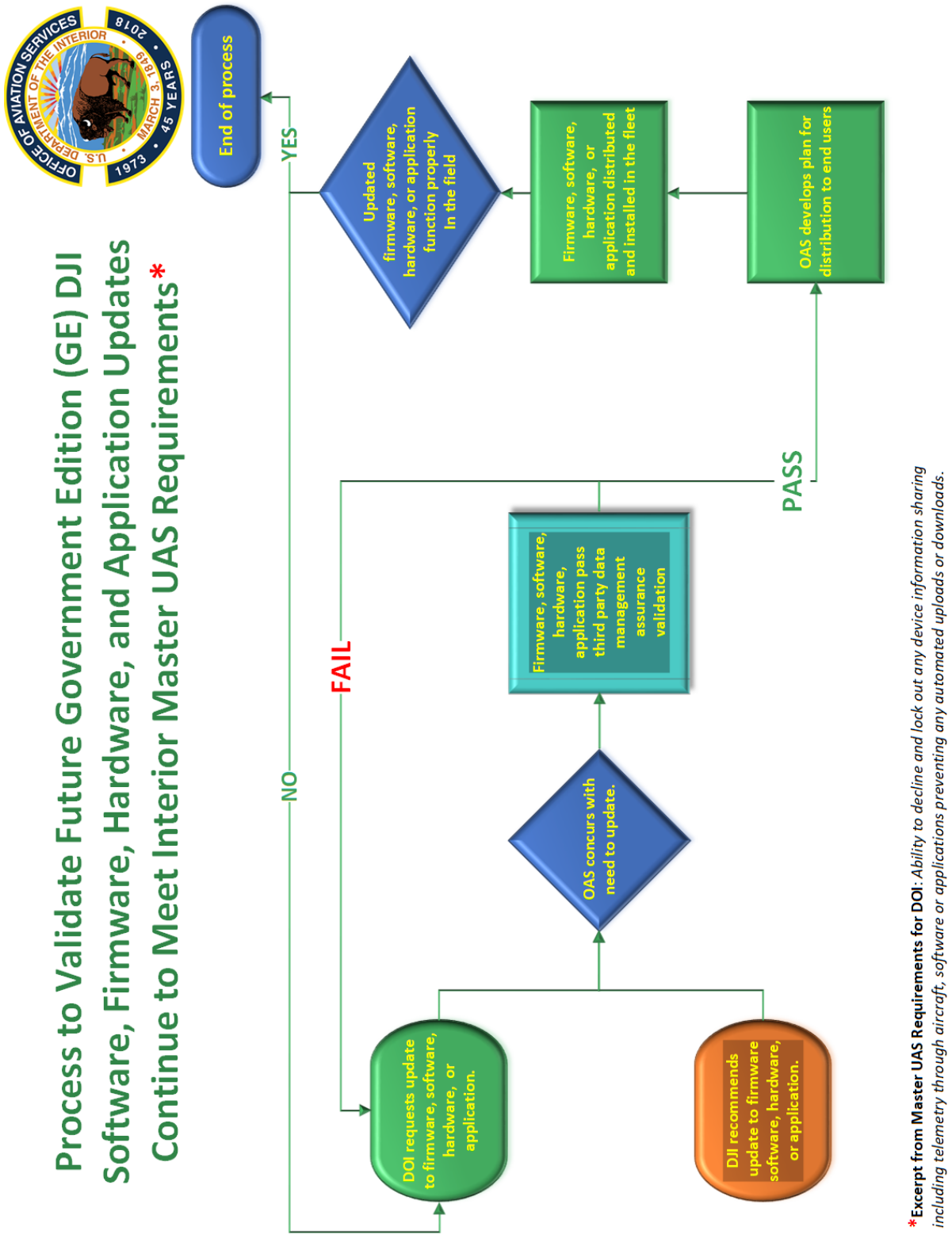
Appendix D - Evaluation of DJI's Specialized Systems for DOI by Drone Amplified, Inc.

OAS Motto:

Appendix A - Government Edition (GE) Off-Aircraft Data Security Risk Mitigation Processes and Protocols



Appendix B - Process to Validate Future Government Edition (GE) DJI Software, Firmware, Hardware, and Application Updates Continue to Meet Interior Master UAS Requirements



Test Plan for Validation and Verification of Data Security Software for Employment of DJI UAS Platforms

PURPOSE OF THE TEST – The purpose of this test is to examine the validation, verification, and utility of aftermarket data security software applications in solving known cyber security issues with DJI products[1] for employment across the full range of U.S. Department of the Interior {DOI) missions. The DOI Office of Aviation Services {OAS) will serve as the lead flight test agency under its Departmental Manual {DM) authority and responsibility for ensuring the Department's legal requirements as a Public Aircraft Operator {PAO) as defined in 49 U.S.C. § 40102{a){41) are met.

BACKGROUND – Since the inception of the DOI UAS program in 2006, cyber security has been a foundational requirement for DOI acquired UAS and operations. DOI has always maintained the links employed by the UAS under its operational control {OPCON) possess the same level of encryption as required of any IT system used in the Department. Additionally, the Department required the ability to "opt-in" to any sharing of flight log, telemetry, or mission video, photo, etc. data with hardware or software manufacturers.

In 2015 following a lengthy UAS requirements development process, DOI determined DJI aircraft did not meet Departmental IT security requirements due to the information collected by DJI and users' inability to control this data sharing at an enterprise level. This information was clearly stated in their publicly available privacy policy. This discovery led DOI to seek out alternatives to DJI products. In 2016, the Department of Defense {DOD) and Department of Homeland Security {DHS) conducted technical assessments of DJI products that led them to the same conclusion as DOI had in 2015.

Ultimately, DOI selected the Solo aircraft, built by 3D Robotics to become its primary small multirotor platform. This aircraft has been quite successful having flown nearly 10,000 flights across a wide range of DOI missions. However, due to intense competition from DJI the Solo is no longer being produced. There currently are no domestically produced aircraft that can perform as well as the DJI aircraft at a comparable price. It is in the best interest of DOI to find a solution that will empower the use of these inexpensive, yet powerful tools for Departmental missions. OAS has been working separately with DJI, DOD and other industry partners to find a solution that is secure, reliable, and available at the enterprise level and will enable OAS to integrate DJI hardware into the DOI Fleet, while meeting cyber security requirements. DOI now has multiple tools at its disposal that achieve this goal. Some provided by DOD and some provided by contractors. This test plan will outline the steps OAS is going to take to conduct operational test and evaluation of these solutions.

REFERENCES:

1. Program Manager, Navy & Marine Corps Small Tactical Unmanned Aircraft Systems {PMA-263) letter of May 24, 2017: Operational Risks with Regards to DJI Family of Products
2. Naval Air Systems Command DJI Cyber Mitigation Data Package of August 8, 2017. FOUO.
3. U.S. Immigration and Customers Enforcement, Homeland Security Investigations SAC Intelligence Program Los Angeles – Intelligence Bulletin of August 9, 2017: Da Jiang Innovation {DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government – LES

Test Plan

SCOPE OF THE TEST – This plan is limited to the testing of provided applications from the Department of Defense (DOD).

TEST ARTICLES – Test articles for this assessment will be limited to the DJI Matrice 600 Pro and Mavic Pro aircraft. Other than the DOD provided software, the aircraft employed in these tests will be commercially representative.

TEST ENVELOPE – All test flights will be flown in accordance with DOI aviation policy for unmanned aircraft as outlined in Operational Procedures Memorandum 11 {OPM-11) and all applicable DM's. The flights will remain with current DOI authorizations for flight in Class G airspace and Temporary Flight Restrictions {TFR), as applicable. Test flights will be conducted away from any known sources of significant electromagnetic interference {e.g. commercial radio, TV antennas, FAA or military radars).

FLIGHT CLEARANCE – Flight clearance is given under the authority of the OAS Director as the senior Interior aviation official and in keeping with OAS's responsibility to ensure the Department meets its legal obligations as a PAO under 49 U.S.C. § 40102{a){41). This flight clearance is solely for the test articles, scope of the test, and flight envelope described above. This signed test plan will serve as the public aircraft declaration, authorizing flight testing of these modified aircraft. The signed test plan will also serve as the Project Aviation Safety Plan {PASP) for this flight series.

METHOD OF TEST – Flight tests will be conducted using a buildup methodology that gradually increases risk, based on the successful completion of previous test flight exit criteria. If exit criteria are not met, the test team will cease operations until a thorough examination of the incident can be accomplished and they receive written OAS Director approval to continue. Likewise, if during the test team believes a modification to the test plan is necessary based on observed results, they will cease operations until the OAS Director can be briefed and his permission is received for any modification to the test plan. Test flights will be designed to closely match the normal conduct of DOI UAS mission flights.

TESTS PHASES

PHASE 1 {OAS testing)

Test Tasks – Obtain needed hardware and software for initial testing.

- Acquire M600 Pro platform.
- Acquire Mavic Pro platform.

- Receive App from DOD and Drones Amplified.

Required Exit Criteria

Apps are validated by DOD as sufficient from a security standpoint - no data transfer.
Apps connect to the UAS as advertised.
Functionality of the apps is as expected.

Phase 2 {OAS Operational Testing)

Test Tasks:

- Field testing of full functionality of the aircraft using secure GCS software {minimum of 12 takeoffs and landings).
    - Arming
    - Takeoff
    - Climbs
    - Turns
    - Range
    - Endurance
    - Speed
    - Comm Link
    - Emergency Procedures
    - RTL
    - Manual Landings
    - Auto landings
- Field testing of Ignis aerial ignition payload on M600.
    - Install and bench test payload.
    - Drop **inert** spheres for 3 cycles to ensure no anomalies.
    - Drop **live** spheres to ensure full function of the payload.
        - Goal is 2500 spheres but is subject to weather constraints.
    - Successful test deploy aircraft with OAS operators to conduce **live** burn with Bureaus. This requires purchase of second M600 for backup.

- Field Testing of Mavic Pro
    - Arming
    - Takeoff
    - Climbs

- Turns
- Range
- Endurance
- Speed
- Comm Link
- Emergency Procedures
- RTL
- Manual Landings
- Auto landings
- Use of goggles

Required Exit Criteria

Hardware/Software perform as expected.
No unexplained anomalies that affect the safety of flight or performance of the aircraft.

PHASE 3 {Bureau Operational Testing)

TEST TASKS:

- Identify with bureaus the number of M600 and Mavic Pro aircraft they would like to acquire NTE 10 M600 Pro and NTE 20 Mavic Pro Aircraft.
- OAS will configure the aircraft with the secure apps and provide the bureau with the aircraft and tablet in the secure configuration.
- Bureau operator will sign an agreement that the will only operate the aircraft in the secure configuration and will make no modifications without OAS approval.
- Bureaus will deploy aircraft for mission work over a 3 month period.
- OAS will monitor usage and provide technical support to bureaus as needed.

Required Exit Criteria

Agreement between OAS/Bureaus that the solutions are a viable fix and are sustainable over time.

PERSONNEL REQUIREMENTS – All personnel operating DOI UAS in support of this plan will be fully qualified and current in accordance with OPM-11.

RISK MANAGEMENT – Safety is the practice of risk management and avoidance of hazards, in accomplishing a task, in order to avoid injury, damage, or loss of resources. Hazards are conditions that are a prerequisite to a mishap. Risk is an expression of possible loss in terms of hazard severity and hazard probability. Risk management is the application of numerical ratings or value judgement to the weighing of risks against the controls necessary to minimize these risks. The test team will employ risk management during each phase of the test to mitigate hazards and the potential loss associated due to a mishap.

TEST PLAN AMENDEMENT PROCEDURE – If the test plan needs to be changed after it has been approved, the test team will brief the OAS Director, describing the background, need, additional risk mitigation, and expected results associated with the requested test plan change. All test plan changes will be memorialized in a signed addendum describing the details of the requested and approved change.

REPORT REQUIREMENTS – The project is not complete until a final report summarizing the tests conducted and results achieved is drafted, submitted to, and accepted by the OAS Director. Interim verbal/email reports are encouraged during the course of the test. OAS Director notification following the completion of each test phase and always when something unexpected occurs.

Test Plan Talking Points

1. DOI's Office of Aviation Services {OAS) has been selected by DOD to serve as a "trusted agent" for this examination.
2. This is a limited test while we sort out additional solutions, including working with DJI on a long term fix.
3. We collaborated with DOD and are acting as beta testers for them prior to this solution being released to a larger governmental community.
4. This is a crawl, walk, run approach.
5. For now, we cannot share with other federal operators. Eventually DOD will open up to a larger group.
6. We cannot share this technology with cooperators until DOD gives the green light.
7. Potential insider threats will be mitigated through signed agreements and mobile device management processes.
8. There is no manufacturer support of these aircraft as part of the program.
9. Bureaus need to understand that there is a potential that these systems may not be approved for long-term use.
10. OAS will conduct train-the-trainer for bureau pilots, providing specific operator endorsements for these aircraft for the purposes of these tests

Test Communications Plan

1. OAS will develop/collaborate with OS/DAS PRE Comms personnel on a press release regarding the test program.
2. OAS will coordinate with DOD on any media inquiries to ensure DOD OPSEC is maintained.
3. OAS will provide regular updates to DAS-PRE on the progress and results of the tests.

BRADLEY KOECKERITZ
Digitally signed by BRADLEY KOECKERITZ
Date: 2018.04.09 10:34:21

MARK BATHRICK
Digitally signed by MARK BATHRICK
Date: 2018.04.09 10:42:38 -06'00'

Submitted Recommending Approval

Brad Koeckeritz
OAS Unmanned Aircraft Systems Division Chief

Approved

Mark Bathrick
Director, DOI Office of Aviation Services

United States Department of the Interior Office of Aviation Services

300 E. Mallard Dr., Ste 200
Boise, Idaho 83706-3991

In reply refer to:

November 14, 2018

Memorandum

To: Mark Bathrick, Director, Office of Aviation Services

From: Brad Koeckeritz, Division Chief Unmanned Aircraft Systems, Office of Aviation Services

Subject: Modification 1 to the Data Management and Security Test Plan

As you are aware, we are ready to move into phase 3 of the test plan utilizing DJI aircraft. Originally we picked a number of 10 M600 Pro and 20 Mavic Pro aircraft. When we approached the Bureaus about what their demand was to participate in the testing program the interest was stronger than originally anticipated. We would like to modify the test plan to increase the number of test article aircraft to 20 M600 Pro and 30 Mavic Pro aircraft. This will allow us to meet the bureau demand while getting a more thorough evaluation of the platforms from a wider user group. The bureaus are aware that there is a possibility that these aircraft may be grounded if there if there are any security concerns.

-X-Approved --Disapproved

MARK BATHRICK

Digitally signed by MARK BATHRICK
Date: 2018.11.16 12:57:31 -07'00'

Mark Bathrick
Director

Office of Aviation Services

United States Department of the Interior

Office of Aviation Services

300 E. Mallard Dr., Ste 200
Boise, Idaho 83706-3991

November 16, 2018

MODIFICATION TWO -Test Plan for Validation and Verification of Data Security Software for Employment of DJI UAS Platforms

This modification expands the original **Scope of Test** to include UAS and associated applications equipped with DJl's Private Edition (aka Government Edition) software, firmware, and hardware bundle. Approved Test Articles remain the DJI Matrice 600 Pro and the Mavic Pro aircraft, fitted with either the previously software or the OAS approved Private/Government Edition.

Mark L Bathrick Director

Office of Aviation Services

Evaluation of DJI's specialized systems for the Department of the Interior

Drone Amplified, INC

Carrick Detweiler and Evan Beachly

{carrick|ebeachly}@droneamplified.com

September 14, 2018
Last updated November 27, 2018

Contents

1 Executive Summary

Charge. We have conducted an evaluation of specialized systems that DJI has designed for the Department of the Interior (DOI). These systems consist of specialized Android and iOS apps for flying DJI drones, a specialized Windows program for configuration and firmware updates, and specialized versions of the Matrice 600 Pro and Mavic Pro drones. The purpose of this evaluation is to determine if the systems leak data to DJI servers under certain operational conditions, and to determine the degree the systems can be operated without connecting to the internet, including the use of the IGNIS payload. Additionally, we test that the specialized drones cannot connect to the publicly-available versions of DJI software.
Update 11/27/2018: DJI has updated some of the specialized systems for DOI, and we've tested whether the systems resolve the issues mentioned in this report. Places in this document where the updated systems have addressed an issue are noted with an italicized note about the update, like this.

Major Findings. Our evaluation process found:

1. The specialized software did not leak data under the investigated operational conditions.

2. The Android and iOS apps make a query to a Domain Name System (DNS) server to resolve the IP addresses of "www.dji.com" when first started. The DNS Server reponds to the query by telling the app the IP addresses of several servers with that domain name. One of the apps then pings one of those servers. This ping does not contain any data, but it could inform the DJI server of the user's IP address, and the time the app was started.

Update 11/27/2018: The app no longer pings the DJI server.

3. All of the features tested on the specialized systems could be used without connecting to DJI servers. In particular, the activation of the DJI Onboard Source Development Kit and specialized DJI Mobile Source Development Kit for Android did not require an internet connection.

4. The specialized version of DJI Assistant (a Windows program for configuring DJI drones) was missing nearly all of the features of the normal version. It only had the capability to update the firmware of the DOI drones.

Update 11/27/2018: An updated version of the specialized version of DJI Assistant now includes the features necessary to support custom payloads.

5. The IGNIS payload works with the specialized DOI Matrice 600 Pro and the specialized version of our Ignis app for Android. However, due to the inability to configure the DOI Matrice 600 pro with DJI Assistant, we had to make some small changes to IGNIS's programming for it to work. These changes to IGNIS will be unnecessary if the configuration features are added to the specialized version of DJI Assistant.
Update 11/27/2018: This is no longer an issue with the updates to the specialized version of DJI Assistant.

6. With the exception of a few small bugs, all of the features provided by the specialized Android and iOS flight apps we tested were functional with the specialized Matrice 600 Pro, specialized Mavic Pro, and with a normal Matrice 600 Pro.

7. Publicly available DJI Software was not able to connect to the specialized DOI Matrice 600 Pro. However, DJI Go 4 and other publicly-available flight apps for iOS and Android were able to briefly connect to the DOI Mavic Pro, and get video, status, GPS position, and potentially more information. Since these apps are not secured, they could leak this data.

Update 11/27/2018: An updated firmware for the DOI Mavic Pro fixes this issue and prevents these publicly-available apps from getting video, status, and GPS position information from the drone.

Recommended changes to the DJI software. We recommend asking DJI to resolve these issues:

1. Add the missing features to DJI Assistant. At a minimum, it needs the Tools tab and the SDK tab. Without these tabs, the support for custom payloads on the Matrice 600 pro is limited.

Update 11/27/2018: The tools and SDK tabs have been added.

2. Remove DNS query and ping to DJI server made by the flight apps. There is no good reason for the apps to do this.

Update 11/27/2018: The app no longer pings DJI servers.

3. Make the DOI Mavic not able to briefly connect to the public flight apps.

Update 11/27/2018: An updated Mavic firmware fixes this issue.

4. Fix the small bugs described later in this report.

Recommended usage practices. Following these practices will mitigate the chances that data will leak, and still grants full functionality of the systems:

1. Train pilots to not use the publicly-available DJI apps with the DOI drones, as the DOI Mavic was able to connect and potentially leak data.

Update 11/27/2018: The issue with the DOI Mavic has been resolved, but we still recommend not installing or running the publicly-available flight apps on a mobile device that will be used with DOI drones.

2. Use the specialized Ignis app to fly DJI drones. The Ignis app implements a firewall that blocks all network communication by the DJI Mobile SDK, providing an additional level of security against data leakage. Additionally, it does this in a way that still allows you to download satellite maps for use during flight.

3. Use the DJI Pilot Beta Private app (the specialized Android app) for configuration. There are a few drone operations that can only be performed by the DJI Pilot Beta Private app (such as configuring video transmission settings, and IMU calibration). Use this app while blocking its network access by disabling WiFi and mobile data on the tablet to ensure it won't leak data. Force stop the app after usage to kill the background processes that would normally persist after closing it.

2 Background

DJI has developed specialized versions of their software and firmware to meet the strict data security requirements of the Department of the Interior. These special versions are expected to not contact DJI servers, nor require contact with DJI servers to use their features.
The software includes custom versions of the DJI GS Pro app for iOS and the DJI Pilot app for Android (which provide an interface to control the drone during flight and view the camera feed), the DJI Mobile SDK for Android and iOS (which allows for the creation of custom flight apps), and the DJI Assistant Windows application (which allows for more advanced configuration of the drone than is possible in the apps).
DJI has also created special versions of their Matrice 600 Pro and Mavic Pro drones with custom firmware that has looser flight restrictions and no requirement to contact DJI Servers for activation. As an additional security requirement, only the specialized software should be able to connect to these specialized drones.

We evaluated these specialized DJI products by checking for data leakage, and checking that the main features could be used without connecting to the internet. Table 1 lists the versions of the software and firmware of the specialized systems for DOI that were tested during our evaluation. Table 3 lists the versions of the software and firmware of the publicly- available DJI systems used for some of our tests.

Specialized Software/Firmware	Operating System	Version
GS Pro DOI	iOS	1.8.2 (SUPPORT-BETA-7)
DJI Pilot Beta Private	Android	v0.6.3pe
Android Mobile SDK	Android	4.6-doi
DJI Assistant	Windows	v00.00.0606
Flight Controller Firmware	Mavic Pro	04.02.44.03
Flight Controller Firmware	Matrice 600 Pro	04.02.41.01

Table 1: Versions of the specialized systems evaluated in this document

Specialized Software/Firmware	Operating System	Version
GS Pro DOI	iOS	1.8.2 (SUPPORT-BETA-8)
DJI Pilot Beta Private	Android	v0.7.3pe
DJI Assistant	Windows	DOI-9-5
Flight Controller Firmware	Mavic Pro	05.00.0134
Remote Controller Firmware	Mavic Pro	05.00.0131

Table 2: Versions of the updated specialized systems evaluated by 11/27/2018 updates

Publicly-available Software/Firmware	Operating System	Version
DJI Go 4	iOS	4.1.18
DJI Go	Android	3.1.43
Litchi	Android	4.8.0-g
DJI Assistant 2	Windows	v1.1.2-2
Flight Controller Firmware	Matrice 600 Pro	03.02.41.13

Table 3: Versions of the public DJI systems also used for parts of the evaluation

3 Data Leakage Tests

We captured the internet traffic during nominal usage of DJI's specialized systems for the Department of the Interior, and analyzed the traffic to determine if the systems contacted DJI servers during that usage. This kind of test cannot prove that the systems won't contact

DJI servers, as the software might only transmit data during conditions that are infeasible to test.

3.1 Flight Apps

3.1.1 Methodology

There are three specialized flight apps that we tested: DJI GS Pro DOI (iOS), DJI Pilot Beta Private (Android), and Ignis (an Android app created using the specialized DJI Mobile SDK). Each app was tested with three DJI drones: a DOI Mavic Pro with the special firmware, a DOI Matrice 600 Pro with the special firmware, and a regular Matrice 600 Pro. The versions of these systems can be found in Tables 1 and 3. The regular Matrice 600 Pro was included because each app is supposed to also be usable with the non-specialized DJI drones.

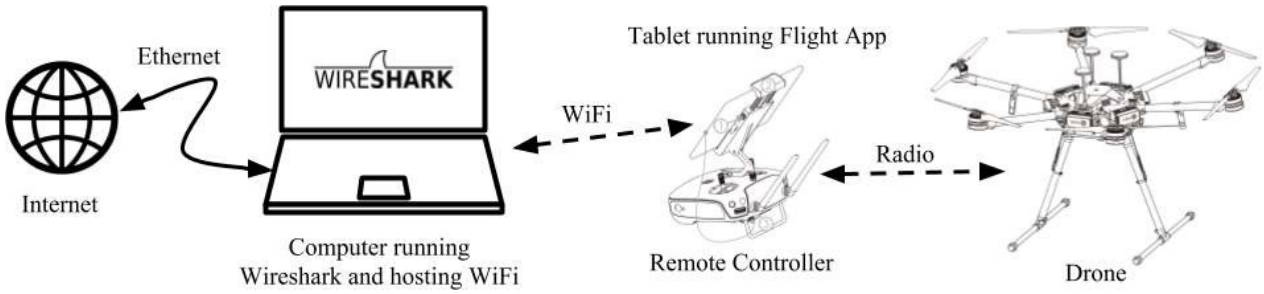


Figure 1: Data leakage test setup

Figure 1 shows the setup of the equipment used for the test. A computer connected to the Internet via an ethernet cable was used to host a WiFi hotspot, and ran Wireshark to capture all internet traffic on the WiFi network. Wireshark is a network protocol analysis program that can capture and interpret all packets transmitted or received on a network (more info at https://www.wireshark.org/). An iPad Air 2 and a Samsung Galaxy Tab A were used to run the flight apps. Each combination of flight app and drone were tested, for a total of nine tests.

Before each test, each app on the tablet was force stopped to ensure that no unnecessary background processes were running. The tablet was connected to the hosted WiFi hotspot, and the other tablet's WiFi was turned off so that only the tablet being tested was on the WiFi network. These steps were taken because the test will capture all network traffic on

the WiFi network, not just the traffic generated by the app that's being tested, and we want to minimize the other traffic in order to simplify analysis.
The test begins by starting the capture of network traffic on the WiFi network by Wire- shark. Then we turn on the app, the drone's remote controller, and the drone. We connect the tablet to the remote controller via a USB cable, and wait until a connection between the drone and the app is established. For the flight, we take off and ascend to 40 feet above ground level, then fly 40 feet out. Next, we manually fly the drone through some maneuvers, such as yawing, circling, and moving side to side, in order to verify that the app is tracking the drone's position on the map. After this, we let the drone hover for 3 minutes, then return to the takeoff point and land. Finally, we turn off the drone, turn off the controller, close the app, and stop capturing network traffic with Wireshark.
Update 11/27/2018: We tested updated versions of DJI GS Pro DOI (iOS) and DJI Pilot Beta Private (Android) using a similar setup with the DOI Mavic Pro and DOI Matrice 600 Pro. However, in these tests we merely started the app and connected the drone, and did not do any flying, as we were looking to verify that the apps do not make a DNS request or ping to DJI servers when they are started.

3.1.2 Results

We analyzed the captured network traffic by looking up every IP address the tablet communicated with during the test. Tables 4, 5, and 6 show some representative examples of the IP addresses contacted during each app's test. Note that these tests capture all network traffic from the tablet, not just the app. There are many packets sent to Apple and Google which are likely sent by the tablet's operating system.

Hostname	IP Address	Location	Notes
Computer hosting WiFi	10.42.0.1	NE	DNS query for www.dji.com
e14868.dsce9.akamaiedge.net	23.64.158.84	MA	Akamai (Maps)
e6987.a.akamaiedge.net	23.204.176.87	MA	Akamai (Maps)
e6987.a.akamaiedge.net	23.45.198.246	MA	Akamai (Maps)
usdal4-vip-bx-002.aaplimg.com	17.253.3.202	CA	Apple
service2-st11-a.ess.apple.com	17.173.255.33	CA	Apple

Table 4: Examples of IP Addresses contacted while using GS Pro DOI app

The GS Pro DOI app uses Apple maps to display maps, and the map tiles are downloaded from Akamai servers.

Hostname	IP Address	Location	Notes
Computer hosting WiFi	10.42.0.1	NE	DNS query for www.dji.com
d125tdjigxzobs.cloudfront.net	143.204.158.117	WA	Ping to www.dji.com
api.mapbox.com	143.204.154.206	WA	Mapbox
android.l.google.com	172.217.9.14	CA	Google
googleapis.l.google.com	216.58.194.42	CA	Google

Table 5: Examples of IP Addresses contacted while using DJI Pilot Beta Private app

The DJI Pilot Beta Private app and Ignis app use Mapbox to display maps, which will download map tiles from their Amazon AWS servers.

Hostname	IP Address	Location	Notes
Computer hosting WiFi	10.42.0.1	NE	DNS query for www.dji.com
events.mapbox.com	52.21.125.0	WA	Mapbox
events.mapbox.com	34.197.191.199	WA	Mapbox
dfw28s04-in-f2.1e100.net	172.217.12.34	CA	Google
dfw25s13-in-f10.1e100.net	216.58.194.74	CA	Google

Table 6: Examples of IP Addresses contacted while using Ignis app

We did not detect any leakage of data to DJI servers with any of the apps. However, all three apps make a Domain Name System (DNS) request to the computer hosting the WiFi network to resolve the IP address of "www.dji.com" when they are first started. This DNS request goes to the router or a DNS server, and does not actually communicate with any DJI servers, but it does tell the app the IP address of DJI servers.

The DJI Pilot Beta app follows this DNS request up with a ping to one of the DJI servers, and receives a ping response back. This ping is used by the app to check that the server is up and can receive messages. The ping does not contain any data, but the server could get the IP address of the tablet and the time the app was started (since that's when the ping is sent).

The special Mobile SDK used by the Ignis app also attempts to ping a DJI server, but the ping is blocked by a firewall built into the Ignis app. The firewall did not block the DNS request, due to the way the firewall was implemented as a virtual private network.

These DNS requests and pings aren't leaking flight data to DJI servers, but there's no good reason for the apps to do them. At best, it's just something DJI forgot to remove when they were creating these versions for DOI. At worst, it's informing the app of DJI servers that it could potentially leak data to.

Update 11/27/2018: The updated version of the DJI Pilot Beta app for Android no longer makes the DNS request nor ping. The updated version of the GS Pro DOI app still made a DNS request, and did not ping one of the DJI servers.

3.2 DJI Assistant

3.2.1 Methodology

We tested the DOI version of DJI Assistant with three drones: a DOI Mavic Pro with the special firmware, a DOI Matrice 600 Pro with the special firmware, and a normal Matrice 600 Pro, for a total of three tests. The normal Matrice 600 Pro was included because this version of DJI Assistant is also supposed to be usable with the non-specialized DJI drones. We connected a Windows 10 computer to the internet over WiFi, and ran Wireshark on it so we could capture all of the computer's network traffic. We closed all other software and killed as many non-essential background processes as we could to minimize network traffic from sources we weren't interested in.

The test begins by starting the capture of the computer's network traffic by Wireshark. Then, we start DJI Assistant, turn on the drone, and connect the drone to the computer with a USB cable and wait for DJI Assistant to recognize the drone. After this we click on the device in DJI Assistant to go to the device's page, and wait 5 minutes in order to collect any network traffic DJI Assistant might send while it is connected to the drone. Finally, we disconnect and turn off the drone, close DJI Assistant, and stop capturing with Wireshark. The version of DJI Assistant that we tested only had the ability to update the firmware of the drone, and did not include the other features and tabs available in the public version of DJI Assistant 2. Most relevant to this test is the Flight Data tab, which can put the drone in SD Card Mode so that the flight logs stored on the drone's SD card can be accessed. It's doubtful that the version of DJI Assistant we tested even has access to the flight logs on the drone without this feature, so it's unlikely that our methodology would see any flight data being leaked.

3.2.2 Results

We analyzed the captured network traffic by looking up every IP address the computer communicated with during the tests. Table 7 shows some representative examples of the IP addresses contacted during the tests with each drone. Note that these tests capture all network traffic from the computer, not just from DJI Assistant. There are many packets

sent to Microsoft, which are likely sent by the operating system or background processes.

Hostname	IP Address	Location	Notes
e-0009.e-msedge.net	13.107.5.88	WA	Microsoft
dm3p.wns.notify.windows.com.akadns.net	13.89.220.65	WA	Microsoft
onecollector.cloudapp.aria.akadns.net	52.114.74.45	WA	Microsoft
vs.login.msa.akadns6.net	131.253.61.82	WA	Microsoft
a1165.dscw19.akamai.net	184.24.97.65	MA	Akamai

Table 7: Examples of IP Addresses contacted while using DJI Assistant

We did not detect any communication to DJI servers.

4 Functionality Tests

4.1 Flight Apps

We tested some of the main functions of the apps to verify that they work with each drone. Some of the apps do not implement certain functions, and those are marked as "Not Possible" or "Not yet implemented".

The Waypoints test evaluated the ability to create a waypoint mission by touching the map to place waypoints, uploading those to the drone, and having the drone automatically fly that mission. The GS Pro DOI app implements some more structured mission types that were not tested. The DJI Pilot Beta Private app has a button to create missions, but it is not implemented yet.

Table 8 shows the results of the tests with the DOI Mavic Pro.

Test	GS Pro DOI	DJI Pilot Beta Private	Ignis
Connecting to Drone	Good	Good, but must start app before connecting USB	Good
Status Information	Good	Good	Good
Set Lost Link Procedure and RTH altitude	Not Possible	Good	Good
Camera Feed	Good	Good	Good
Manual Flight beyond 50m and above 30m	Good	Good	Good
Auto Takeoff, Auto Landing	Not Possible	Not Possible	Good
Waypoints	Good	Not yet implemented	Good
Set max flight altitude up to 1000m	Not Possible	Good	Not Possible
Take pictures, Start/Stop Recording	Good	Good	Good
Adjust Exposure, Focus, Camera Mode	Good	Good	Good
Calibrate Compass	Good	Good	Good
Calibrate IMU	Not Possible	Good	Not Possible

Table 8: DOI Mavic Pro functionality tests

Normally, the maximum flight altitude of a DJI drone is limited to 500 meters, but the DOI versions can raise that limit to 1000 meters. However, the Android Mobile SDK used by the Ignis app was not able to set the max flight altitude above the normal value of 500 meters on the DOI drones. Fortunately, the DJI Pilot Beta Private app is able to set the max altitude above 500 meters, and then the setting will persist on the drone when used with the Ignis app.

Tables 9 and 10 show the results of the test with the DOI and Regular Matrice 600 Pro.
The Matrice 600 Pro has a few more functionalities than the Mavic, which we tested.
The “Camera Feed (Zenmuse)”, “Take pictures, Start/Stop Recording”, and “Adjust Exposure, Focus, Camera Mode” tests on the Matrice 600s were tested with a Zenmuse X5 Camera.

Test	GS Pro DOI	DJI Pilot Beta Private	Ignis
Connecting to Drone	Good	Good, but must start app before connecting USB	Good
Status Information	Good	Good	Good
Set Lost Link Procedure and RTH altitude	Not Possible	Good	Good
Camera Feed (Zenmuse)	Good	Good	Good
Camera Feed (HDMI)	Good	Intermittent	Good
Manual Flight beyond 50m and above 30m	Good	Good	Good
Auto Takeoff, Auto Landing	Not Possible	Not Possible	Good
Waypoints	Good	Not yet implemented	Good
Set max flight altitude up to 1000m	Not Possible	Good	Not Possible
Take pictures, Start/Stop Recording	Good	Good	Good
Adjust Exposure, Focus, Camera Mode	Good	Good	Good
Move Gimbal in app	Not Possible	Not possible	Good
Recenter Gimbal with C1 and C2	Not Possible	Good	Good
Calibrate Compass	Good	Good	Good
Calibrate IMU	Not Possible	Good	Not Possible
Communicate with Onboard SDK	N/A	N/A	Good

Table 9: DOI Matrice 600 Pro functionality tests

Configuring the DOI Matrice 600 Pro to reliably display video from an HDMI camera with DJI Pilot Beta Private is not trivial and we could only get the video feed to intermittently work on Android. We tried multiple different setting configurations to get the camera to work reliably, but were unable to determine a pattern of why it sometimes worked and sometimes didn't. Sometimes a configuration would result in good video, but would not work the next time the camera was connected.

Update 11/27/2018: The Ignis app has been updated with the ability to configure the video feed settings, and using these we were able to reliably configure the DOI Matrice 600 Pro to display video from an HDMI camera in the Ignis app. However, even with that exact same configuration, the DJI Pilot Beta Private app would not display the video.

Importantly, we were able to do all of these tests with the DOI drones without

needing to connect to the internet. We did not need to connect to the internet to register the Android Mobile SDK for the first time, nor connect the DOI Matrice 600 to DJI Assistant to activate the Onboard SDK.

The DOI Matrice 600 was able to allow communications with the IGNIS payload, which uses the DJI Onboard SDK to communicate with the Ignis app through the drone. However, since we could not use DJI Assistant to configure the drone's baud rate and reduce the number of packets it sends, we had to make some changes to IGNIS to match the default baud rate of the Matrice 600 (230400) and handle the large quantity of packets sent by the drone.

Test	GS Pro DOI	DJI Pilot Beta Private	Ignis
Connecting to Drone	Good	Good, but must start app before connecting USB	Good
Status Information	Good	Reports IMU as Abnormal	Good
Set Lost Link Procedure and RTH altitude	Not Possible	Good	Good
Camera Feed (Zenmuse)	Good	No video feed	Good
Camera Feed (HDMI)	Good	No video feed	Good
Manual Flight beyond 50m and above 30m	Good	Good	Good
Auto Takeoff, Auto Landing	Not Possible	Not Possible	Good
Waypoints	Good	Not yet implemented	Good
Set max flight altitude up to 500m	Not possible	Good	Good
Take pictures, Start/Stop Recording	Good	Good	Good
Adjust Exposure, Focus, Camera Mode	Good	Good	Good
Move Gimbal in app	Not possible	Not possible	Good
Recenter Gimbal with C1 and C2	Not possible	Good	Good
Calibrate Compass	Good	Good	Good
Calibrate IMU	Not possible	Good	Not Possible
Communicate with Onboard SDK	N/A	N/A	Good

Table 10: Regular Matrice 600 Pro functionality tests

The DJI Pilot Beta Private app had a few issues when used with a regular Matrice 600

Pro. It reports the IMU as Abnormal, and the video feed was black. Strangely, a few minutes into the "Camera Feed (Zenmuse)" test, the edges of objects started to appear in the video feed as grey lines.

4.2 DJI Assistant

As mentioned earlier, the specialized version of DJI Assistant that we evaluated only had the capability to update the firmware of the drone, as shown in Figure 2. It is missing many of the features available in the publicly available version of DJI Assistant 2, such as configuring the PWM and SDK outputs. We did not test updating the firmware, as the test cases in the Test Case report document included with the specialized software for DOI already contained thorough test cases of this firmware update feature, and reported successful results.

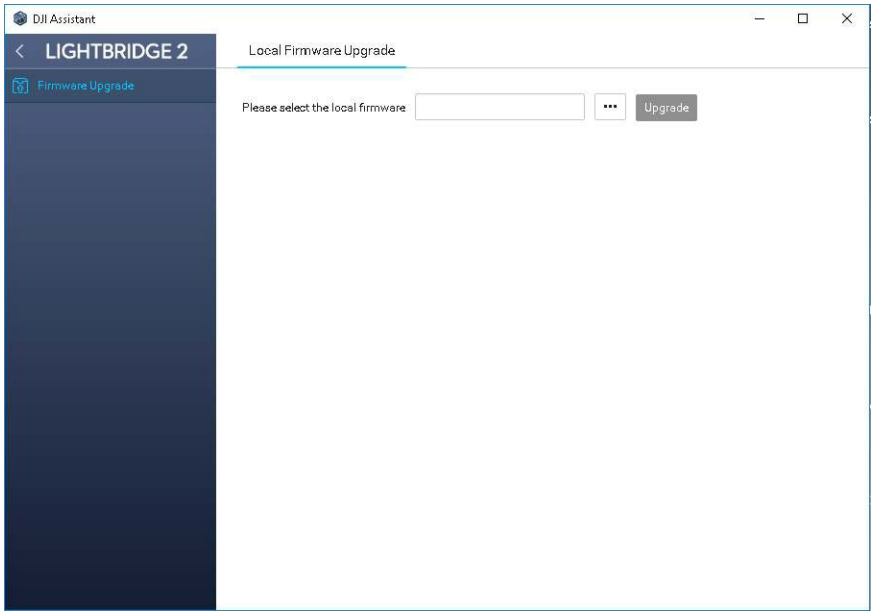


Figure 2: A screenshot of DJI Assistant when connected to the DOI Matrice 600

Update 11/27/2018: A new version of the specialized version of DJI Assistant added the Tools and SDK tabs, and we were able to configure the PWM and SDK settings of the DOI Matrice 600 for the IGNIS payload, and verified the full functionality of IGNIS.
Additionally, we successfully updated the firmware of the DOI Mavic Pro flight controller and remote controller using this version of DJI Assistant. However, the first time we tried updating the flight controller firmware, we encountered an ambiguous "Upgrade failed" error. The cause was an insufficient battery charge on the Mavic Pro's battery (it was at 38%).

Replacing the battery for one at 75% allowed the upgrade process to start.

5 Incompatibility Tests

There's an additional requirement that the DOI drones should not be able to connect to the publicly available DJI software. We tested connecting to the two drones with the official DJI Go app for Android and iOS, Litchi (a 3rd party Android app), and DJI Assistant 2. The results are in Table 11.

Software	DOI Matrice 600	DOI Mavic
DJI Go (Android)	Does not connect	App stops responding
Litchi (Android)	Does not connect	Connects briefly, then disconnects
DJI Go (iOS)	Does not connect	Connects briefly, then disconnects
DJI Assistant 2	Does not connect	Does not connect

Table 11: Incompatibility tests between the DOI drones and the publicly available, unsecured DJI software

Litchi (Android) and DJI Go (iOS) were able to briefly connect to the DOI Mavic, and could get the status of the drone and its GPS position, and some of the video feed before disconnecting. Litchi on Android disconnects almost immediately, but DJI Go 4 on iOS would stay connected and get live video for up to 5 seconds. Figure 3 shows a screenshot of DJI Go 4 on iOS when connected to the DOI Mavic.

Figure 3: A screenshot of DJI Go 4 on iOS connected to the DOI Mavic

Update 11/27/2018: We tested connecting DJI Go 4 (iOS) and Litchi (Android) to the DOI Mavic with the updated firmware, and the app would disconnect immediately. No video, status, or position information from the drone was displayed in the app.

6 Recommendations

6.1 Changes to DJI Software

We recommend asking DJI to make the following changes:

1. **Add the missing features to DJI Assistant.**

The specialized version of DJI Assistant we evaluated could only be used to update the drones' firmware. At a minimum, it needs the Tools tab and the SDK tab that are available in the public version of DJI Assistant 2. Without these tabs, the support for custom payloads on the Matrice 600 pro is limited.

Update 11/27/2018: The Tools tab and SDK tab have been added.

2. **Remove DNS query and ping to DJI server made by the flight apps.**

All three apps made for DOI make a DNS request to resolve the IP addresses of

"www.dji.com" when they are started. DJI Pilot Beta Private and the Android app made with the special version of the Android Mobile SDK for DOI both follow the DNS request up with a ping to one of DJI's servers. No data is transmitted, but there's no good reason for the apps to do this.

Update 11/27/2018: DJI Pilot Beta Private no longer makes a DNS request for "www.dji.com" nor pings a DJI server. DJI GS Pro DOI still makes the DNS request. An upcoming version of the Android Mobile SDK may fix this behavior in the app built with the SDK.

3. **Make the DOI Mavic not able to briefly connect to the public flight apps.**
   Public flight apps such as DJI Go and Litchi are able to briefly connect to the DOI Mavic, and get video feed, position, and status. This has the potential to leak flight data to DJI Servers, as these apps are not secured.

Update 11/27/2018: The updated firmware for the DOI Mavic fixes this issue.

6.2 Bug fixes

There are also a few bugs we would like to recommend asking DJI to fix:

1. **Fix the video feed from normal Matrice 600 Pro to DJI Pilot Beta Private app.**
   The DJI Pilot Beta Private app shows a black video feed when used with a normal Matrice 600 Pro. This issue can be worked around by using the GS Pro DOI app for iOS, or the Ignis app for Android.

Update 11/27/2018: This bug still exists.

2. **Fix the HDMI video display from DOI Matrice 600 Pro to Android apps.**
   The DOI Matrice 600 Pro could not be easily configured to reliably display video from an HDMI camera. This can be worked around by using Zenmuse cameras.

Update 11/27/2018: The Ignis app can now configure the DOI Matrice 600 Pro to transmit video from an HDMI camera, and display the video in the app. The DJI Pilot Beta Private app still could not display the video from an HDMI camera.

3. **Add the ability to set the max flight altitude up to 1000m in the Mobile SDK.**
   The special Mobile SDK used by the Ignis app can only be used to set the max flight altitude up to the normal 500 meters, but the DOI drones support going up to 1000 meters. This can be worked around by using the DJI Pilot Beta Private app to set the max flight altitude.

Update 11/27/2018: An upcoming version of the special Mobile SDK may fix this bug.

6.3 Usage

We recommend taking these steps to mitigate the chances that data won't leak:

1. **Train pilots to not use the publicly-available DJI apps with the DOI drones.**
   The publicly-available DJI apps were able to briefly connect to the DOI Mavic and get status, video, and position information, and could potentially get more information. Until this issue is resolved, the best course of action is to train the users to not use the publicly-available DJI apps.

Update 11/27/2018: The issue with the the DOI Mavic has been resolved, however we still do not recommend installing or using the publicly-available flight apps on a mobile device that will be used with DOI drones.

2. **Use the Ignis app to fly DJI drones.**

The Ignis app implements a firewall that blocks all network communication by the DJI Mobile SDK, providing an additional level of security against data leakage. Addition- ally, it does this in a way that still allows you to download satellite maps for use during flight.

3. **Use the DJI Pilot Beta Private app for configuration**

There are a few drone operations that can only be performed by the DJI Pilot Beta Private app (such as configuring video transmission settings, and IMU calibration). Use this app while blocking its network access by disabling WiFi and mobile data on the tablet to ensure it won't leak data. Force stop the app after usage to kill the background processes that would normally persist after closing it.

7 About Drone Amplified

Drone Amplified is a small and focused company on drone enabling technology. It was founded in 2015 by Dr. Carrick Detweiler and Dr. Sebastian Elbaum. Both are Computer Science faculty members and founded the Nimbus Lab at the University of Nebraska - Lincoln, an advanced laboratory developing more robust and reliable UASs to enable interactions with the environment. Dr. Detweiler received his Ph.D. in 2010 from MIT in Electrical Engineering and Computer Science with a focus on robotics. Since joining UNL he has focused on developing sensors, systems, and algorithms for field robot systems. Dr. Elbaum received his Ph.D. in 1999 from the University of Idaho. He is the recipient of multiple grants from NSF, including an NSF CAREER Award, and a Google Award, aimed at developing anal- ysis techniques to make software systems more dependable at a lower cost.

Among Drone Amplified's most well known products is *Ignis*, a system that enables drones to assist in fire management through autonomous ignition and monitoring. Ignis has been integrated with a several drones, including DJI's drones, for which we have developed multiple interfaces through software and hardware, and flown extensively for the over 2 years. This report builds, in part, on this experience and in our expertise in drone systems and their analysis.