Issue/Topic

Key Messages and FAQ's: OAS Flight Test and Technical Evaluation Report on the Completed 15-Month Unmanned Aircraft System (UAS) Data Management Assurance Evaluation

Key Messages

1. OAS and DOI are recognized leaders in UAS safety, management, and application: 2017 Commercial Drone Alliance Industry Heroes Award, 2018 Samuel J Heymann Service to America Medal finalist, Commercial UAV News Top 7 Visionaries, >600 drones, >400 pilots, >20,000 flights, millions in documented savings, zero public complaints, unprecedented documentation and transparency.

2. DOI also led the way in UAS mission and security requirements and best practices; only agency with published Master UAS Requirements, only one to include a data management requirement to *"to decline and lock out any device information sharing including telemetry through aircraft, software or applications preventing any automated uploads or downloads."*

3. OAS just completed a groundbreaking collaboration and an accompanying 15-month professional flight test and technical evaluation program now provides DOI bureaus with access to inexpensive, highly capable, and data secure UAS that support critical wildland fire, SAR, emergency response, and natural resources applications. Also available to other agencies.

FAQ's

Q: What prompted DOI to undertake this initiative?

A: Drones are an increasingly critical tool for Interior bureaus in safely, effectively, efficiently, and responsively carrying out their mission responsibilities. Drone use by DOI bureaus increased 563% from FY16 to FY17 and 108% from FY17 to FY18, with over 20,000 UAS flights to date. In 2016, Interior awarded its first competitive commercial fleet UAS acquisition contract to 3D Robotics (3DR), an American company, who's UAS were manufactured in China. The 3DR Solo UAS met all DOI's mission and data management assurance requirements. Although DOI acquired over 450 drones from 3DR, they stopped building drones shortly after contract award due to a number of factors, including market pressure from other drone companies. This initiative was part of Interior's UAS Integration Strategy which emphasizes ongoing market research and collaboration with industry, academia, and government partners to maintain Interior's cutting edge leadership in the domestic application of this technology. As the Department's aviation experts, OAS regularly collaborates with industry to educate them on Interior requirements and assess potential solutions for current and future needs. As DJI currently commands an estimated 70% worldwide market share in the commercial drone sector, it made sense to include them in these efforts. In turn, DJI expressed a desire to understand and meet DOI's Master UAS Requirements.

Q: Why did DOI look at foreign manufactured drones?

A: Currently, all commercial drones are either manufactured in China or include electronic components manufactured there. <u>DOI's fleet of over 600 drones includes models from **U.S.** companies (3D Robotics, BirdsEyeView) and a **French** company (Parrot)</u>. The <u>Department of Defense recently selected the Parrot to take part in the development of next-generation short range reconnaissance drone</u> for the U.S. Army.

Q: Didn't the Department of Homeland Security (DHS) warn companies back in May that data may be at risk if they used DJI drones?

A: No. DHS never specifically called out DJI in that industry alert. DHS's alert applied to "Chinese Manufactured UAS." DOI's fleet of over 600 drones includes models from **U.S.** companies (3D Robotics) and a **French** company (Parrot) - <u>ALL manufactured in China</u>. Interior's Office of Aviation Services not only assisted DHS with the development of best practices to reduce risk listed in the document, <u>but employed them since the inception of DOI's current UAS program in 2006</u>.

Q: What experience does DOI have in testing drones and cybersecurity?

A: This flight test and technical evaluation program was developed and carried out in accordance with accepted military flight test and DOD test and evaluation methods and practices; <u>OAS's Director has 30+ years' experience in every facet of military experimental test flying and flight test management</u> and is Defense Acquisition Workforce Improvement Act (DAWIA) Test and Evaluation Level III (top level) certified.

For the data management assurance assessment, DOI collaborated with a proven industry partner (Drones Amplified) OAS had previously contracted to conduct cyber security testing; they successfully identified a data leak. DOI also enlisted the assistance of partners at NASA and another federal agency and their national laboratory partner (note: they have asked to remain unnamed). Both agencies, performed the data assurance tests and confirmed the security of the Government Edition software and firmware that was specifically developed for Interior.

Q: What was the extent of Interior's testing?

A: Interior conducted over **2,200** individual test flights across a wide range of DOI missions as part of the evaluation. These included:

1. <u>Volcano response and monitoring</u>: Gas detection, assessment, and monitoring. <u>Crater mapping</u>. Lava flow speed determination.
2. <u>Search and Rescue</u> (SAR).
3. Prescribed fire area inspections.
4. <u>Aerial ignition</u> 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. <u>Emergency equipment delivery</u> (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.

The tests followed a formal test plan signed by the OAS Director and each DOI UAS pilot who participated read and signed the test plan.

Q: The report indicates Interior tested a DOD solution. Why wasn't that used?

A: While the DOD solution was secure, it provided insufficient mission functionality for DOI bureaus' complex photogrammetry, mapping, etc. mission data requirements.

Q: What were the conclusions of the report?

A: (1) the final tested version of DJI Government Edition (GE) provided a reasonable mitigation for known data management assurance vulnerabilities of the stock Matrice 600 Pro and Mavic Pro UAS, **(2)** Test results could not be projected to future GE versions, **(3)** residual risk could be further mitigated by employing the two tested UAS only on missions that collect non-sensitive, publicly releasable data, and **(4)** market research found no domestically available alternatives that are competitive in **price**, required mission and security **performance**, and necessary **scalability** to the two tested UAS.

Q: What were the report's recommendations?

A: (1), Approve the acquisition of M600Pro and Mavic Pro aircraft in the Government Edition configuration **(2)**, Maintain third party validation of any new or updated software, firmware, hardware, or ancillary DJI applications **(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 <u>DOI and DHS UAS Best Practices for Responsible Operations</u>, and **(5)** Continue ongoing work between OAS, DOI bureaus, OCIO, industry and federal partners to identify long-term UAS data management assurance solutions.

Q: Exactly what did Interior authorize as a result of the report?

A: <u>DOI may acquire and operate DJI Matrice 600 Pro and Mavic Pro aircraft specially configured with GE (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5) as part of the DOI UAS fleet</u>. No updates to the currently approved DJI hardware, firmware, and software are permitted without subsequent OAS approved third party validation and contingent on positive results, written OAS Director authorization. Bureaus should limit use of these aircraft to non-sensitive missions whose UAS collected data is publicly releasable.

Q: Does this mean DOI will be buying DJI drones now?

A: Not necessarily. ALL DOI UAS acquisitions are conducted through full and open public contract solicitations that outline specific requirements. All drone manufacturers that meet the stated performance requirements are eligible for consideration. Warranted and aviation experienced contracting officers with the Department's Interior Business Center Acquisition Services Directorate (not part of OAS) make the contract award selections.

Q: Isn't Interior worried about the use of foreign manufactured products?

A: Interior believes agencies should treat all technology as if it's a potential security risk, regardless of where it or its component parts are manufactured. As we have seen over recent years, data security breaches have occurred in both U.S. government and corporate arenas.

Q: How does Interior's decision to authorize these two DJI drones for acquisition and limited use align with the administration's views on trade with China and concerns over security?

A: The two drones included in this limited authorization have already demonstrated their unique ability to fulfill the mandates of the President's Executive Order on promoting active management of federal lands to reduce wildfire risk. In particular, the approved M600 Pro has been used extensively to conduct hazardous fuels reduction, burnout operations during wildfires, enhancing firefighter safety and effectiveness. The M600 provides the first-ever night aerial ignition capability, able to operate when the fire is most vulnerable. In supporting prescribed burns prior to fire year, the M600 aerial ignition drone provides greater safety and flexibility over traditional helicopter methods, which have claimed six lives and resulted in the loss of three helicopters in the last 14 years.

Q: How does this effort align with the Buy America Act (BAA), the Trade Agreements Act (TAA), and the President's July 15, 2019 Executive Order (EO) on Maximizing Use of American-Made Goods, Products, and Materials.

A: Warranted and aviation experienced contracting officers with the Department's Interior Business Center Acquisition Services Directorate (not part of OAS) make all Interior aviation contract award selections. Interior's contracting processes ensure compliance with the provisions and exceptions of the BAA and TAA. Interior will comply with the EO as soon as implementing regulations are drafted and received from the Office of Management and Budget.

**Q: Why didn't Interior just use Department of Defense drones instead of pursuing commercial drones?**

A: In 2008, Interior acquired $25M worth of excess DOD small UAS (at no cost) for operational test and evaluation (OT&E) in support of DOI UAS Master Requirement's development. As a result of this extensive OT&E effort from 2010 to 2014, Interior found that DOD drones did not meet DOI bureau requirements for sensor resolution and versatility, product processing capabilities, and compatibility with operations within the continental U.S. (radios). DOD drones were also 10-100X more expensive than commercial alternatives; unaffordable by DOI bureaus.

Q: Didn't the Department of Defense ban DJI drones?

A: The Army directed units to discontinue the use DJI drones on August 2, 2017. Of note, these were stock DJI drones that Interior had previously determined did not meet our data assurance management requirements in 2015 (and never authorized for Interior bureaus). The Army memo was overridden by a May 23, 2018 memo from the Deputy Secretary of Defense that acted on a May 14, 2018 DOD IG report finding that DOD had not implemented an adequate process to assess cyber security risks associated with using commercial-off-the-shelf (COTS) UAS. As a result, DOD suspended the use of all COTS UAS, unless exempted. DOD has already granted several exceptions to this ban.

Q: What additional steps has Interior taken to ensure data security when using DJI drones?

A: For all its drones, Interior employs a "layered security" approach. This approach provides multiple, independent risk mitigation measures that together provide a high level of assurance. This diagram illustrates this model and the measures employed for the two authorized DJI drones
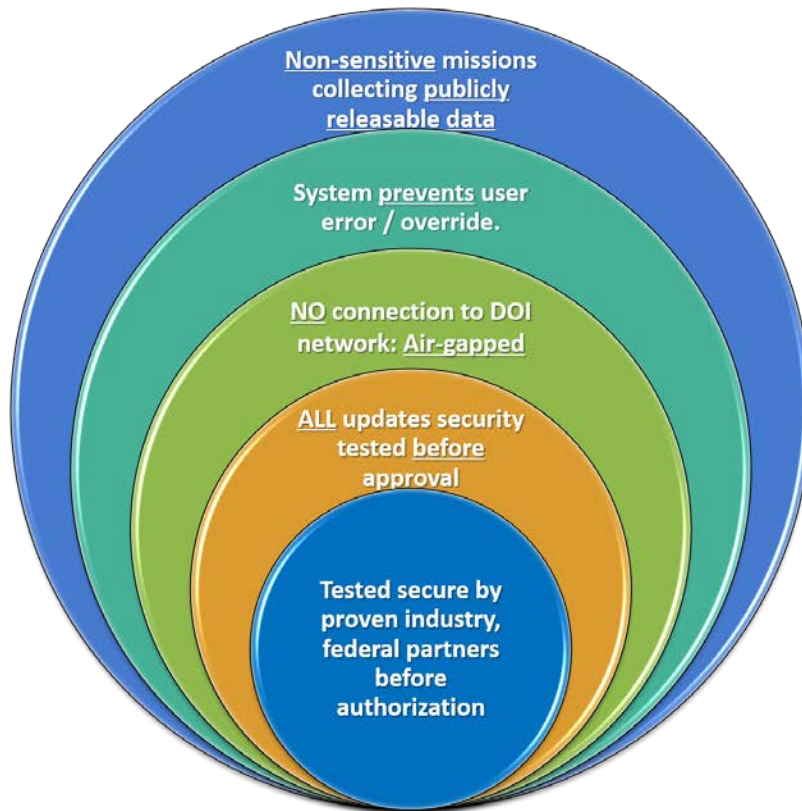
Q: As a result of this report and the subsequent authorization, are other agencies using DJI drones?

A: Yes. The National Oceanic and Atmospheric Administration (NOAA) has authorized their principle investigators to begin procuring the two specially configured drones tested by DOI. U.S. Forest Service has also indicated their desire to procure these specially configured drones through OAS in support of wildland firefighting operations.

Q: The report says this is an "interim solution." What is a long-term/permanent solution?

A: 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. A preferred long term solution would have the following characteristics: (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.

Point of Contact

Mark L Bathrick, Director, OAS: mark_bathrick@ios.doi.gov.