



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

3/17/2021

Mr. Eric Lander
Director-Designate
Office of Science and Technology Policy
Executive Office of the President
Washington, DC 20504

Dear Mr. Lander:

This letter is in response to a request from your office to the Department of the Interior (DOI, Department, or Interior) on March 5, 2021, for specific information related to the reporting requirements of Executive Order 13981. Answers to the specific questions about unmanned aircraft systems (UAS) are provided below and in the enclosed spreadsheet.

1. A brief explanation of how Interior plans to prevent the use of taxpayer dollars to procure UAS that present unacceptable risks and are manufactured by, or contain software or critical electronic components from, foreign adversaries, and to encourage the use of domestically produced UAS.

The Department plans to prevent the use of taxpayer dollars to procure UAS that present unacceptable risks and are manufactured by, or contain software or critical electronic components from, foreign adversaries. Interior also encourages the use of domestically produced UAS, which has been a founding tenet of the Department's UAS program since its inception in 2006. Specific actions undertaken by the Department to achieve these goals include:

- a. DOI Mission and Operating Environment Risk Assessment.** In assessing risk levels, Interior first examined its mission and operating environment, which is almost completely "benign"—the lowest risk among UAS operating environments. The Department of Defense (DOD) defines benign environments as: "*(i) . . . a public venue that will not expose any sensitive facilities, equipment, or activities before, during, or after the event. (ii) All information or data generated . . . is approved and appropriate for public release.*"^{1,2} The land DOI manages fits this definition in numerous ways. DOI manages over 500 million acres of public land.³ While Interior enforces restrictions on

¹ U.S. Air Force, *USAF Process For Requesting Exemption To DEPSECDEF Ban On Commercial Off The Shelf (COTS) Unmanned Aircraft Systems (UAS)*, No Date.

² DOI, <https://www.doi.gov/sites/doi.gov/files/uas-emergency-readiness-waiver-form-2020-12-10.pdf>

³ DOI, <https://www.doi.gov/sites/doi.gov/files/migrated/pmb/osdbu/upload/dbwdoi.pdf>

aircraft taking off or landing on certain DOI lands (e.g. National Parks, some refuges), most DOI lands are not restricted from commercial or private drone takeoff and landing operations, and only 0.006 percent of the airspace above DOI-managed lands is restricted by the Federal Aviation Administration (FAA) from overflight by manned or unmanned private or commercial aircraft. Additionally, DOI-managed public lands are routinely open to both foreign and U.S. visitors. According to the 2018 Interior Economic Report, 486 million foreign and U.S. visitors came to DOI lands in 2018.⁴ No DOI public lands currently prohibit public photography; images of Interior lands are widely available online through multiple public, commercial, and government sources. Likewise, Interior's Earth Explorer website offers over 6.4 million frames of photographic images available for public download as medium- and high-resolution digital products. The available high-resolution data supports photogrammetric quality scans of aerial photographs and include many taken from DOI UAS.

Thus, the overall risk levels are low given Interior's unique, mostly benign operating environment and near-total access to the public. In 2020, DOI required bureaus to track and report the environments in which their UAS operated; 99 percent (3,255) of DOI UAS flights occurred in "benign" environments as defined by DOD. Interior estimates 98 percent of the 33,288 UAS flights flown by the Department since 2010 have been in benign environments.

- b. Development and Incorporation of Technical Security Requirements.** Interior was the first Federal agency to implement publicly posted UAS technical specifications that included requirements for DOI enterprise control over any data sharing with UAS platform, payload, or software processing manufacturers.⁵ As a result, Interior was never exposed to the data sharing risks of other agencies that initially allowed the unregulated procurement of stock commercial UAS products. Interior's UAS technical specifications mandate all UAS incorporate password-protected encrypted flight control and sensor/payload links. No Interior UAS are allowed to connect to the DOI enterprise network, and all mission data is physically transferred from the UAS to relevant government data processing equipment where it is subjected to the same standard virus and malware scans as other external data.
- c. Implementation and Oversight of Layered Policy and Programmatic Risk Mitigation Measures.** Interior's UAS program employs a layered system of policy and programmatic risk mitigation measures that complement its technical security requirements. Only UAS approved by Interior's Office of Aviation Services (OAS) may be procured. OAS ensures each UAS is registered with the FAA, inventoried, and configured before it is assigned to one of Interior's bureaus. All updates, payload changes, and modifications to Interior UAS must be approved by OAS. OAS developed and provided oversight of Interior's UAS Operator training and qualification course that includes instruction on UAS security requirements and personal accountability. Only

⁴ DOI, <https://www.doi.gov/sites/doi.gov/files/uploads/fy-2018-econ-report-final-9-30-19-v2.pdf>.

⁵ DOI, Office of Aviation Services, https://www.doi.gov/sites/doi.gov/files/uploads/doi_master_uas_requirements_document_-_v1.3_3-15-19.pdf.

Interior personnel who have successfully completed the Department’s UAS Operator training and qualification course are permitted to operate Interior UAS. OAS conducts program oversight through regular UAS operator check flights, UAS integrity inspections, and unit program evaluations. For operations involving the two built-to-DOI specification Da-Jiang Innovations Government Edition (GE) UAS (Mavic Pro and M600 Pro), OAS has limited their use to non-sensitive missions that collect publicly releasable data.

- c. Collaboration with Industry and Interagency Partners to Develop and Test UAS that Conform to DOI UAS Security Requirements.** Interior has consistently collaborated with industry to field UAS that conform to DOI UAS security requirements and the DOI mission risk profile. In July 2019, OAS completed a 15-month, 2,245-flight, comprehensive and collaborative test and technical evaluation program to field the first built-to-DOI specification GE UAS to meet previously unfulfilled bureau wildland fire and scientific mission demands. To evaluate the risk mitigation measures of the two GE models, OAS enlisted one industry and two Federal partners. Early in the process, OAS requested DOD’s participation as a partner testing agency but was informed that current DOD priorities did not afford it the ability to support testing at that time. OAS worked closely with the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS-CISA), which contracted with the Department of Energy’s Idaho National Laboratory (INL) to conduct an information security risk evaluation of four UAS flown by DOI, including the two built-to-DOI specification GE aircraft. The October 2019 DHS CISA & INL evaluation report executive summary stated that “...there are no major areas of concern related to data leakage, thereby supporting that the multi-layered mitigations DOI has in place (including the use of built-to-specification GE software, firmware, and hardware) are in fact working as designed to meet their published security requirements.”⁶ Likewise, the industry (Drones Amplified) and another Federal partner (National Aeronautics and Space Administration) independently came to the same findings. In response, OAS granted a limited authorization for DOI bureaus to operate the GE aircraft, limiting their operations to non-sensitive missions where collected UAS data was publicly releasable. OAS also restricted the use of GE aircraft to the specifically tested configuration and prohibited any updates without follow-on testing and subsequent approval by OAS.
- d. Ensuring all DOI UAS Contracts Conform with the Federal Acquisition Regulations and Provisions (FAR) of the Buy American Act (BAA).** All DOI aircraft procurement and service contracts are managed by warranted contracting officers (COs) from the Interior Business Center’s Acquisition Service Directorate, which is under the oversight of the Interior Property and Acquisition Management Office. Interior COs ensure each contract complies with the provisions of the FAR and BAA. OAS has consistently worked closely with American drone manufacturers, providing them with publicly posted, detailed technical specifications for DOI UAS requirements, issuing and supporting numerous formal requests for demonstration, and remaining open and

⁶ INL, *Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation*, INL/LTD-19-55545, Revision 2, October 2019.

available to coordinate meetings with OAS and bureau partners to answer their questions about Interior's UAS mission needs and technical specifications. Of Interior's current fleet of 853 UAS, 59 percent (504) were purchased from U.S.-based companies.

Based on comprehensive and robust actions taken by the DOI UAS program, Interior believes it has encouraged the use of domestically produced UAS while also mitigating the risk of using currently available and mission-compatible UAS to a low, acceptable level.

2. Explain the security risks posed by Interior's existing Federal UAS fleet and outline potential steps that could be taken to mitigate these risks.

The National Institute of Standards and Technology (NIST) and DHS CISA have both emphasized the importance of sound technical requirements in establishing a risk-managed cybersecurity framework. Interior's UAS security program is based on a multi-layered, overlapping, requirements-based approach. As a result, DOI UAS have conducted over 35,000 flights since 2006 with no identified data security compromises.

Notably absent from the NIST Framework for Improving Critical Infrastructure Cybersecurity (version 1.1, April 16, 2018) is any mention of country-of-origin bans as an effective cybersecurity strategy. Country-of-origin based product bans can actually reduce security and increase the risk of undetected data breaches by giving non-covered countries (e.g. Vietnam, India, Singapore, etc.) a "free-pass," that could provide an opening for nefarious actors to target these open commercial supply chains for infiltration and compromise. Interior believes the security risks posed by the existing DOI UAS fleet is **low**. This is supported by an assessment of the threat posed by Interior's mission and operating environment, the potential vulnerabilities of the UAS employed, and the positive steps and layered measures Interior has taken to mitigate potential risks, previously described above.

3. Explain the operational impact to Interior if ordered to discontinue use of all Federal covered UAS.

In fiscal year (FY) 2020, Interior experienced firsthand the scope of impacts such an order would cause. On October 30, 2019, the then Secretary grounded all DOI UAS and stopped all planned UAS acquisitions and training classes. On January 29, 2020, this action was formalized in Secretary Order (SO) 3379. Since October 30, 2019, only "Emergency Operations" UAS flights were permitted. This resulted in a cessation of all DOI science, climate change research, and natural resource management UAS operations, contributing to a nearly 70-percent decline in DOI UAS flights in FY 2020. In the wildland fire mission, the combined effect of the grounding, the resultant cancellation of nearly 200 planned UAS procurements and 224 operator training classes—coupled with the chilling effect of the required waiver and reporting process—resulted in a 64-percent reduction in FY 2020 UAS support to wildland fire when compared to FY 2019; this is despite a 117-percent increase in acres burned in FY 2020. If ordered to discontinue use of all Federal covered UAS, the impacts across a broad spectrum of Department missions and Administration priorities would increase from what the Department has experienced to date under SO 3379.

While 59 percent of DOI's UAS fleet of 853 aircraft were sourced from U.S.-based companies and another 21 percent from companies based in allied countries, 100 percent of the UAS fleet were manufactured in or contain significant components manufactured in a foreign adversary country. This is not only the reality of today's worldwide commercial UAS market, but that of many other consumer and professional electronics, specifically cell phones, TVs, cameras, smart speakers, computers, and computer monitors.

UAS Are Essential to Emergency, Natural Hazard, and Research Missions—Saving Lives, Improving Employee Safety, and Dramatically Reducing Department Costs.

Since 2010, Interior has successfully flown 33,288 UAS flights across more than 30 different mission applications. Approximately 68 percent were flown in support of science-related missions. Representative Interior missions that will be impacted by an order to discontinue use of all Federal-covered UAS include, but are not limited to: (1) wildland fire prevention and response; (2) climate change research; (3) flood monitoring and response; (4) volcano research and eruption response; (5) earthquake response; (6) hurricane response; (7) search and rescue; (8) endangered species monitoring; (9) landslide prediction monitoring, and response; (10) oil and gas lease monitoring; surface mine reclamation and monitoring; (11) cultural and archeological resource identification and monitoring; oil spill response; (12) avalanche research; (13) wildlife monitoring; (14) habitat monitoring; and (15) invasive species monitoring.

DOI has publicly documented the measured success of its UAS program in official reports and positive news articles. In 2017, a published report estimated that the discovery of an otherwise unobserved spot fire by an Interior UAS resulted in saving more than \$50 million in land and infrastructure value. In 2018, a DOI UAS was instrumental in guiding a lost resident and responding emergency personnel away from a fast-moving lava flow to effect the resident's rescue during the Kilauea eruption, saving lives. DOI's publicly posted 2018 and 2019 Annual UAS Summary Reports documented annual operational savings of \$14.8 million and \$15.7 million respectively through the use of UAS versus traditional means of carrying out the same missions.^{7,8}

With their ability to carry sensors capable of 1,200 times the resolution of LandSat and OAS' qualification of 37 different sensors for DOI UAS, they have proven their ability to provide superior science over many traditional methods and offer unique and easy opportunities for public transparency. The use of UAS has also improved employee safety. UAS have been used to replace the requirement for manned helicopters in aerial ignition operations. Since 2005, the Federal fire community has experienced six fatalities and the loss of three helicopters, due to crashes during aerial ignition missions, the latest occurring in 2019. UAS have enabled Interior to remove employees from potentially hazardous terrain, flooding, volcanic eruption, noxious gas, and animal threats without compromising the mission. UAS have also delivered significant procurement, training, maintenance, and infrastructure savings

⁷ DOI, https://www.doi.gov/sites/doi.gov/files/uploads/doi_fy_2018_uas_use_report.pdf

⁸ DOI, <https://www.doi.gov/sites/doi.gov/files/uploads/fy19-flight-use-report-2020-03-24.pdf>

to resource-constrained bureaus and missions. The average per-aircraft cost of the current DOI UAS fleet is \$2,100, with a total fleet cost of less than \$2 million. UAS have likewise delivered more responsive service, often with an ability to more quickly deploy than traditional contracted or fleet-manned aircraft. If ordered to discontinue use of all Federal covered UAS, the science, safety, savings, and service benefits described above will be lost to Interior and its employees.

There Are No Viable UAS Alternatives that Are Not “Covered UAS”

Currently, there are no viable UAS alternatives that meet Interior bureau mission requirements and would not be characterized as “Federal covered UAS.” The “Blue UAS”, developed by DOD were designed to meet the Army’s Short-Range Reconnaissance (SRR) requirement. SRR vehicle performance specifications do not meet published DOI UAS requirements and those of several models in the current DOI fleet. With only two integral sensors, “Blue UAS” lack the payload performance and modularity present in most current DOI UAS. “Blue UAS” have two fixed sensors—one electro-optical and one thermal infrared. In comparison, the current DOI UAS fleet is able to carry over 37 unique payloads, enabling them to support a wide array of science, natural resources, and wildland fire missions. “Blue UAS” would thus reduce DOI UAS sensor capabilities by 95 percent. In December 2020, Interior initiated a solicitation for each of the five “Blue UAS” models. As part of that effort, DOI’s U.S. Geological Survey (USGS) National UAS Project Office (NUPO) conducted extensive manufacturer-sponsored flight tests of a “Blue UAS” model. NUPO’s seven-page written test report cited aircraft performance concerns in recommending to the Source Selection Evaluation Board against procurement of this aircraft.⁹ The procurement was subsequently canceled.

Beginning on December 18, 2020, Interior required all bureaus to assess and report whether DOI UAS mission flights permitted through the “emergency operations” waiver to the Secretary’s grounding order would have been appropriate for a “Blue UAS.” Of 42 approved DOI UAS projects between then and March 9, 2021, none indicated a “Blue UAS” would have been appropriate for the mission. Blue UAS payload inadequacy was cited in 31 (74 percent) of the projects, while high cost and availability issues were cited in 11 (26 percent). In addition to performance and mission requirement gaps, “Blue UAS” models cost between 8-14 times the average cost of current DOI UAS. This makes them unaffordable for DOI bureaus to use in a scale where the full science, savings, safety, and service benefit of UAS is realized.

Furthermore, the provenance of “Blue UAS” as being free of significant components manufactured by a foreign adversary has come into question. DOD’s FY 2020 Industrial Capabilities Report to Congress stated that *“an analysis of the bill of materials from four randomly selected U.S. sUAS platforms that meet the DoD requirements revealed that*

⁹ USGS National Unmanned Systems (UAS) Project Office, Geosciences and Environmental Change Science Center, *USGS Operational Testing*, January 14, 2021.

certain components rely heavily on Chinese suppliers."¹⁰ The report goes on to state that printed circuit boards were among the top three component categories in which U.S. UAS had the most reliance on parts from China.

4. Explain Interior's plan, if ordered, to expeditiously remove covered UAS from Federal service.

If ordered to expeditiously remove covered UAS from Federal service, OAS would follow existing procedures for the disposal of Federal aircraft. Affected aircraft would be recalled, inventoried, and offered for sale on the General Services Administration Auctions to State, Local, Tribal, and Territorial governments and the general public, none of which have imposed UAS country-of-origin bans. At this time, DOI likely would not procure replacement UAS due to the factors highlighted above.

5. Provide Interior's point of contact for inquiries that includes name, phone number, and e-mail address.

The Interior point of contact is: Mark Bathrick, Director, Office of Aviation Services, (208) 867-6987, mark_bathrick@ios.doi.gov

Sincerely,

RACHAEL
TAYLOR

Digitally signed by
RACHAEL TAYLOR
Date: 2021.03.17
16:53:29 -04'00'

Rachael S. Taylor
Principal Deputy Assistant Secretary
Policy, Management and Budget

Enclosure

cc: Avril Haines, Director of National Intelligence

¹⁰ DOD, Office of the Under Secretary of Defense for Acquisition and Sustainment, *Report to Congress – Fiscal Year 2020: Industrial Capabilities*, January 2021.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
Office of Aviation Services (OAS)¹	480	China	SOLO ² by 3DR, Berkeley, CA, USA	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) Nearly all DOI missions are flown over open public ³ lands in benign ⁴ environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	178	China	ANAFI ⁵ by Parrot, Paris, France	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) Nearly all DOI missions are flown over open public ³ lands in benign ⁴ environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	24	China	FIRFLY6 PRO ⁶ by Birdseyeview Aerobotics, Andover, NH, USA	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) Nearly all DOI missions are flown over open public ³ lands in benign ⁴ environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
<p>OAS</p>	<p>82</p>	<p>China</p>	<p>MAVIC PRO Government Edition (GE)⁷ by DJI, Shenzhen, China</p>	<p>(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data, (f) only DJI MAVIC PRO fitted with the built-to-DOI specification Government-Edition software, firmware, and hardware package (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5), tested and reported on in the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security (DHS-CISA) and Idaho National Laboratory (INL) Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation Report of October, 2019 are approved for use.</p>	<p>No. DOI Owned Fleet Aircraft.</p>

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	78	China	M600 PRO Government-Edition (GE) ⁷ by DJI, Shenzhen, China	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data, (f) only DJI M600 PRO fitted with the built-to-DOI specification Government-Edition software, firmware, and hardware package (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5), tested and reported on in the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security (DHS-CISA) and Idaho National Laboratory (INL) Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation Report of October, 2019 are approved for use.	No. DOI Owned Fleet Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	5	China	EVO by Autel, Shenzhen, China	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) Nearly all DOI missions are flown over open public lands in benign environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	1	China	R1 by Skydio, Redwood City, CA, USA	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and in benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No Owned Aircraft DOI Fleet

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	2	China	Apprentice S 15E by E-flite - Champaign, Illinois, USA ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and in benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	2	China	Loki by Sky-Hero Brussels, Belgium	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	1	China	H10 by DroneVolt - Villepinte, France	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	No. DOI Owned Fleet Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
 Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	2	Unknown ⁸	Argentech FireEye 2 Newmarket, ,NH ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and in benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	2	Unknown ⁸	L3 Harris FVR90 Melbourne, FL ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	2	Unknown ⁸	Silent Falcon Albuquerque, NM	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	1	Unknown ⁸	UAV Factory, Sovenia ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

EO 13981, PROTECTING THE UNITED STATES FROM CERTAIN UNMANNED AIRCRAFT SYSTEMS

Section 3

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	1	Unknown ⁸	Drone America Hugin Air Reno, NV8	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	3	Unknown ⁸	Insitu Scaneagle Bingen, WA	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
 Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	3	Unknown ⁸	Stalker, Lockheed Martin Bethesda, MD, USA ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands and benign environments and 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Call-When-Needed Contract Aircraft

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary
Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
OAS	1	Unknown ⁸	Cobalt 110 Tucson, AZ ⁸	(a) no DOI drones connect to the DOI enterprise network (digital data media is hand-transferred to DOI computers and subject to DOI network scans/protection), (b) DOI retains enterprise data lockout/sharing authority with DOI drone platform, payload, and data processing manufacturers, (c) all DOI drones have separate password encrypted aircraft control and sensor payload links, (d) the DOI Office of Aviation Services (OAS) centrally controls and oversees the selection, distribution, modification, updating, training, and authorized use of DOI drones, and (e) nearly all DOI missions are flown over open public lands in benign environments and approximately 98% of DOI drone missions are non-sensitive, collecting publicly releasable data.	Yes. DOI Contract Aircraft.
Total	868				

¹ In accordance with DOI Departmental Manual 112 DM 12, para 12.2 C. (1), the Interior Office of Aviation Services (OAS) is responsible for managing ownership, acquisition, assignment, and disposal of all DOI owned fleet aircraft.

²3DR is headquartered in Berkley, CA, USA. Their SOLO aircraft were manufactured in China and contain Chinese components.

Reporting Requirements - Foreign-Adversary-Manufactured UAS or UAS with Significant Components Manufactured by Foreign Adversary Currently Owned, Operated, or Controlled by the **U.S. Department of the Interior**

Component	Quantity	Manufacturer (Country of Origin)	Model	Relevant Security Protocols	Controlled by the component through a third-party contractor?
-----------	----------	----------------------------------	-------	-----------------------------	---

³DOI manages over 500M acres of public land, open to U.S. and foreign visitors. None of these public lands currently prohibit photography. According to the 2018 Interior Economic Report, 486M U.S. and foreign visitors recreated on DOI lands. Only 0.0006% of the airspace over DOI managed public lands is restricted from flight by private aircraft and drones. Interior's Earth Explorer website (<https://earthexplorer.usgs.gov/>) offers over 6.4 million frames of photographic images are available for public download as medium and high resolution digital products. The high resolution data provide access to photogrammetric quality scans of aerial photographs.

⁴DOD defines "benign" environments for UAS use as those where: i. The event location is a public venue that will not expose any sensitive facilities, equipment, or activities before, during, or after the event. ii. All information or data generated or collected during the event is approved and appropriate for public release.

⁵Parrot is headquartered in Paris, France. Their ANAFI aircraft are manufactured in China and contain Chinese components.

⁶BirdsEyeView is headquartered in Andover, NH, USA. While the FIREFLY6 PRO is manufactured in the U.S., they contain Chinese components.

⁷Links to: Government-Edition (GE) DHS-CISA Report Posted by the Association of Unmanned Vehicle Systems International [AUVSI]:

<https://www.auvsi.org/sites/default/files/DHS%20report.pdf>, OAS Technical Report:

https://www.doi.gov/sites/doi.gov/files/uploads/oas_flight_test_and_technical_evaluation_report_-_dji_uas_data_management_assurance_evaluation_-_7-2-19_v2.0.pdf, and

OAS Limited Authorization: https://www.doi.gov/sites/doi.gov/files/uploads/limited_dji_uas_authorization_-_final_signed_-_july_3_2019.pdf.

⁸ DOI has a call-when-need (CWN) contract in place with 7 commercial vendors to provide UAS support for wildland firefighting operations. The current contract does not require a comprehensive componentry breakdown and country-of-origin assessment. Recent contact with the vendors in support of this data call indicate most are unsure of the country-of-origin of their printed circuit boards (PCBs). Accordingly, we have labeled the manufacturer country-of-origin as "Unknown" for these aircraft.