DOI UAS Program

Myths vs. Facts

Myth: DOI's UAS Fleet consists of aircraft solely from Chinese companies.	**Fact**: There are 853 aircraft in the DOI UAS Fleet inventory. Of these, 506 (60%) came from American UAS companies. Another 178 (21%) came from a French UAS company. Only 19% of DOI's UAS Fleet comes from China-based companies.
Myth: DOI data has been compromised due to cyber vulnerabilities with its UAS fleet.	**Fact**: DOI has gone to great lengths to develop and implement layered security policies, procedures and protocols to ensure UAS data security. No DOI UAS connect to the Department's IT network and all mission data is hand-transferred, not connected to the internet. DOI also engaged industry partners, DHS CISA/INL and NASA to tested and validate the DJI Government Edition aircraft (GE) met DOI data security requirements. There are ZERO documented instances of DOI UAS data being compromised.
Myth: DOI collects vast amounts of "sensitive" data with its UAS.	**Fact**: The vast majority (<98%) of UAS data collected by DOI personnel is non-sensitive and publicly releasable. In fact, there is a 2015 Presidential memorandum requiring the release of government UAS data to the public whenever possible.
Myth: The DOD did a comprehensive review of the government edition aircraft.	**Fact**: The DOD has never provided OAS with a written report (classified or otherwise) that documents any data

	breaches from the Government Edition aircraft or any other DOI Fleet UAS.
Myth: US industry is able to produce cost effective small UAS that meet DOI operational needs.	**Fact**: Every solicitation the DOI has issued in the life of its program have been full-and-open competition. IF any American UAS manufacturer was able to compete on price and or performance they would have gotten the award in accordance with the Buy American Act.
Myth: The Blue UAS are the solution to a safe and secure source of small UAS.	**Fact**: The Blue UAS are not a replacement for the existing DOI Fleet. They cost up to 10 times currently available commercial UAS and only meet about 20% of the mission set of DOI. As a result, our bureaus have not expressed much interest in them. Additionally, we have asked the vendors repeatedly for demonstrations and only one has been able to show they have a product ready to be widely sold.
Myth: The grounding of the DOI UAS fleet was "temporary."	**Fact**: The previous Administration only allowed for selected emergency type missions to occur. The overall impact was a complete elimination of scientific missions conducted with UAS across DOI. This includes missions such as oil and gas monitoring, climate change research, endangered species surveys, and geological hazard assessments.
Myth: DOI has enough trained personnel and aircraft to meet its UAS needs.	**Fact**: The grounding of the DOI fleet and the subsequent wholesale cancellations of training in FY20 have greatly impacted

	the bureaus. OAS and the bureaus estimate the Department has 300 fewer trained UAS pilots and 400-600 fewer aircraft than it would have had if the grounding order had not occurred.
Myth: The current waiver and reporting process for emergency missions is scalable and efficient.	**Fact**: The current waiver and reporting process for emergency mission UAS flights has had a "chilling effect" on UAS usage within DOI, as evidenced by the precipitous drop in UAS flying in 2020 over what was projected.
Myth: Some UAS are "different" than other types of information technology with respect to cybersecurity.	**Fact**: UAS are nothing more than a flying WIFI network with a camera/sensor attached. If we can secure WIFI routers, cell phones and digital radios (all of which carry foreign components) then we can secure our UAS by establishing and adhering to accepted cybersecurity requirements. Country of origin bans actually reduce security by giving all other origin countries a "free-pass," allowing bad actors to target these policy-based cyber vulnerabilities.
Myth: Banning UAS made in China will help support American businesses.	**Fact**: There are currently 1.7 Million UAS registered in the UAS and 522,000 are commercially operated. 85%+ of those are made by DJI and well over 90% are were manufactured in China by other companies. Banning use of drones made in China effectively kills any opportunity for those small businesses to do work for the government, including collecting non-sensitive publicly releasable data.

Myth: Banning DOI use of Chinese drones enhances security.	**Fact**: If the DOD and DHS really had concerns about security with these aircraft then why would they not be trying to prevent the public from operating them. Simply put, this is not about cybersecurity. It is about the DOD promoting the domestic production of UAS. DOI has the largest non-DOD fleet of UAS in the entire federal government. Our 853 UAS represent 0.15% of the current commercial UAS flying in the national airspace. Is 0.15% of the market really going to be enough to support a robust UAS industry in the United States? There are over 1.7 million UAS registered with the FAA. With some exceptions, the public can operate their aircraft over DOI lands whenever they want. Why would an adversary go to the great lengths of developing a sophisticated system for capturing DOI data when they could simply have someone on tourist visa collect it for them.
Myth: We can switch to US built aircraft with the flip of a switch.	**Fact**: The economic policies of the last 40+ years has led to most of consumer electronics industry being manufactured in China. We simply cannot pivot without some sort of transition period. Our estimate is that it would take 5-10 years to grow the production within the United States to be competitive. That would only happen with robust investment from the government. We are not aware of

	any effort sufficient to drive this change. Consumers and the private sector are always going to got with what works best and is cost effective. Right now, that is not U.S. manufactured UAS.
Myth: Securing UAS data is somehow different from other types of data.	**Fact**: All data can be valuable and should be protected based on its perceived value. We should be setting standards for all data security regardless of how it is collected.
Myth: The DOI Secretarial Order was developed in coordination with DOI aviation leadership.	**Fact**: There was zero communication from the SECDOI to the career aviation professionals in the nine DOI bureaus or at OAS.
Myth: DOI needs the same level of security as DOD.	**Fact**: The mission of the DOI is vastly different than the mission of DOD. We operate over public land, accessible to US citizens and visitors to this country. To apply the same level of security as DOD is unnecessary and wasteful. There are many examples across the Department where we use information technology that the DOD would never use. Cell phones, computers, cameras, radios etc….The consumer off the shelf UAS DOI operates are not designed to be weapons of war. We wouldn't use a predator UAS to make a map and likewise we wouldn't use a COTS UAS in combat. The Blue UAS program may make sense for DHS and DOD. It does not for DOI and the other land management

	and science agencies conducting non-sensitive missions.