WHITEFOX

Enabling the Good While Preventing the Bad:

How Security Enables the Drone Industry

BACKGROUND

WhiteFox Defense Technologies, Inc. ("WhiteFox") is a global leader in drone airspace security and is pioneering the safe integration of unmanned aircraft systems (UAS, or drones) into society. WhiteFox works with many government and UAS industry stakeholders, and is a proud member of the Commercial Drone Alliance. Guided by the benefit of their experience, WhiteFox presents here a path forward for industry and government to work together to accomplish integration of UAS in the National Airspace System ("NAS") while ensuring safety and security.

INTRODUCTION

The benefits of commercial UAS are substantial. Our society is only just beginning to realize the full potential of UAS. In recent years, UAS technology has moved forward rapidly, and what used to be considered toys are quickly becoming powerful commercial and governmental tools that provide enormous benefits in terms of safety and efficiency. In the United States and abroad, UAS are being used every day to save lives, increase safety and enhance economic productivity. Today, public safety agencies, educational institutions and industry utilize UAS for everything from disaster relief efforts to inspecting critical infrastructure to precision agriculture—and everything in between.

But while it is clear that commercial UAS use can deliver significant safety and security benefits to the American people, it is also true that, like any new technology, UAS have the potential to raise safety and security concerns. Recent events, both domestically and abroad, have highlighted the need to protect against potential public safety and homeland security threats posed by UAS. In December 2018, a reported UAS incursion wreaked havoc on Gatwick Airport, the United Kingdom's second-busiest airport, leading to the cancellation of more than a thousand flights over a 33 hour period, reportedly causing at least $64M in immediate damages. The Gatwick authorities were unable to identify the drone in question. A capable UAS detection system would have removed any question about whether a UAS was flying in the airspace near the airport and further, would have assisted authorities in identifying the rogue UAS operator. More recently, in April of this year, a rogue UAS was spotted hovering over Boston's Fenway Park during a Major League Baseball game in violation of a Federal Aviation Administration (FAA) Temporary Flight Restriction (TFR). Meanwhile, small consumer UAS have been used abroad to deliver weapons.

UAS security threats at home and abroad have left regulators grappling with how to address illegal UAS flights, particularly in sensitive airspace surrounding airports, sporting and mass gathering events, and critical infrastructure facilities, while at the same time enabling beneficial UAS uses. Public safety officials have the responsibility to consider all of these issues.

How can society enable the good UAS have to offer, while preventing the bad? WhiteFox offers its thoughts here.

ESSENTIAL BUILDING BLOCKS FOR EXPANDING COMMERCIAL UAS OPERATIONS WHILE ENSURING SAFETY AND SECURITY

To promote innovation, enable expanded commercial UAS operations like beyond visual line of sight (BVLOS) and operations over people, and move the commercial UAS industry forward in the U.S., it is essential to simultaneously protect against potential public safety and security threats posed by UAS. Below are the critical building blocks and concepts for expanding commercial UAS operations while ensuring airspace security in the U.S.

1. Tiered UAS Remote Identification Approach

First and foremost, in order to promote innovation basic “rules of road” for all UAS operators are necessary. To enforce existing laws and rules, law enforcement must have a means of remotely identifying drone operators. And in order to mitigate threats caused by rogue drones, law enforcement must be able to distinguish the “good” from “bad” drones, or friend vs. foe (IFF). The FAA has the ability now to leverage existing technological solutions and establish a comprehensive remote identification framework for all drones over a certain weight threshold in the sky. Given variant levels of risk, this concept must include a tiered and secure approach to UAS remote identification. With technology available now, it is critical that such a framework be adopted swiftly.

Notably, most rogue drone incursions are caused by careless or clueless drone operators—not criminals. With trusted remote identification, law enforcement has an additional tool in the toolbox for education and enforcement. Trusted remote identification introduces accountability into the system, and enables officials to mitigate potential drone threats only when absolutely necessary. A common sense UAS identification system has the following elements:

- **Comprehensive**: The FAA Reauthorization Act of 2018 enabled the FAA to regulate *all* UAS as necessary for safety and security, and this was an important step. A comprehensive remote UAS identification system applicable to all UAS weighing more than 250 grams is essential to promote innovation and establish reasonable controls to protect against potential safety and security threats posed by UAS. Remote identification can only be successful with near universal participation, such that authorities can assume non-participation is itself indicative of a threat. The only exception should be where the airspace is itself designated for special uses, such as at a designated test site or Academy of Model Aeronautics (AMA) flying field.

- **Security**: While a general remote identification standard applicable to all UAS is urgently needed, it is also essential to adopt a tiered approach: Require remote identification security based on the sensitivity of the airspace, operator, or operation. For certain low risk and simple operations, within visual line of sight in unpopulated areas for example, a lower tier non-secure remote identification standard may be appropriate. However, a higher tier secure remote identification solution must be adopted for UAS operating in and around our nation's most sensitive airspace and for more complex expanded UAS operations, like beyond visual line of sight (BVLOS) operations. Without proper security protections, UAS identities can be easily impersonated, forged, or modified without detection at little to no cost. Without security, anyone can forge his or her identity, from any location, by simply broadcasting it. To be clear, there are not degrees of security. Dependent on the airspace, operator, or operation, it is either sufficient for a remote identification to not be trusted—or secure remote ID and tracking is required.

Potential Implementation of a Tiered Remote ID Security Requirement

	Airspace	**Operator**	**Operation**
General Remote ID *Example Baseline*	Rural, Urban, Localities making a "controlled choice", Uncontrolled Airspace	Hobbyist, Low-Risk Commercial	VLOS
Secure Remote ID *Categories of Applicability*	Critical Infrastructure, Mass Gatherings, TFR, Localities making a "controlled choice"	Government, Known Operators Program, Sophisticated Commercial	BVLOS, Vehicle over 55 lbs

- **Flexible:** The remote identification framework must also be flexible and interoperable to support a variety of purposes, ranging from binary actions like Identify Friend or Foe (IFF) to supporting robust UAS Traffic Management (UTM) systems.

- **Ease of Use**: To ensure broad compliance, remote identification must be easy to use, cost-efficient to implement, and immediately deployable. The remote identification solution must also allow for easy retrofitting of the existing millions of UAS.

- **Scalable**: Remote identification must be scalable from individual organizations, such as a critical infrastructure facility, to world-wide deployment. This means the solution must be capable of integrating into existing land-based communications infrastructure and also rapidly deployable where infrastructure does not exist or is destroyed, such as after natural disasters.

2. UTM Will Be a Key Component of Airspace Structure

UTM will be a key component of airspace structure, management, and coordination as more UAS operate in the NAS. UTM will only function with (1) cyber security and (2) levels of trust. Cyber security protections must ensure that a UA cannot spoof the signal it is broadcasting to misrepresent its own identity, thereby allowing a perpetrator to conceal their malicious behavior by identifying as someone else.

With regard to levels of trust, UTM will only be successful if there is a Known Operators Program that enables expanded operations for operators with higher levels of trust based on additional authentication and secure remote identification. The federal government should collaborate with industry to develop a program similar to the Transportation Security Administration's Pre-Check and Global Entry programs, which will support relevant government stakeholders in identifying legitimate threats, while also promoting public trust and improving efficiency. Such a program would also enable the government to maintain a database of authorized commercial UAS operations, which would help the relevant agencies and public safety officials with threat discrimination. Technology must be used to ensure the authenticity of the identities through elevated remote identification security requirements.

3. Counter-UAS Systems Will Enhance Safety and Enable Expanded UAS Operations

Legislators and policymakers must enable the use of counter-UAS technology to mitigate criminal and negligent UAS threats in a way that is surgical, selective, and safe. Counter-UAS systems can help to enhance the safety and security of UAS operations and will be a key component to enabling expanded operations. In basic terms, counter-UAS systems must enable the good while preventing the bad. This will require counter-UAS and UTM systems to co-exist in the same ecosystem. Much in the same way as the highway patrol is critical to safe highways, counter-UAS technology is critical to enabling the highway in the sky. A comprehensive counter-UAS legislative policy framework must include the following elements:

- **Expand Counter-UAS Authority to Certain State and Local Law Enforcement Agencies**: While the counter-UAS authorities granted to certain Federal agencies in recent legislation is a positive first step towards addressing threats posed by unlawful uses of UAS, these federal agencies still do not have broad authority or the resources necessary to protect all sensitive areas from rogue UAS threats. For that reason, it is essential that counter-UAS legislation expand certain counter-UAS authorities to selected state and local law enforcement agencies tasked with protecting sensitive areas from UAS threats, potentially including airports, stadium sporting events, amusement parks, public gatherings, and other critical infrastructure sites. Legislation enabling certain state and local law enforcement agencies to use counter-UAS technology should be guided by the following principles.

- **Establish Clear Criteria for Evaluating Counter-UAS Systems**: Any additional counter-UAS legislation, regulation, or policy should establish a clear conceptual framework for evaluating the safety and efficacy of counter-UAS systems. The evaluation should consider, among other things, the system's ability to operate safely and selectively, and its compatibility with the safe integration of lawful commercial UAS into the NAS.

- **Avoid Interference With Authorized UAS Operations**: Counter-UAS legislation, regulation, or policy must include procedural safeguards to ensure that any mitigating actions are both justified and proportionate to the perceived threat. It should require that the counter-UAS operators exercise due care to use technologies that avoid incidental damage to innocent third-party manned or unmanned aircraft, communications, equipment, facilities, or services. Moreover, whenever possible, counter-UAS operators should be required to make reasonable efforts to provide notice to a UAS operator before taking action, so that authorized and compliant UAS operators have an opportunity to discontinue potentially offending or non-compliant behavior.

- **Require Mandatory Training for Personnel Engaged in Counter-UAS Activities**: To help ensure that the deployment of counter-UAS technologies does not adversely affect authorized UAS flights, threaten privacy, civil rights, or civil liberties, or otherwise cause harm, any new counter-UAS legislation, regulation, or policy must include substantial training and qualification requirements on the safe and authorized deployment of counter-UAS technology for all personnel engaged in counter-UAS activities. Personnel should be required to maintain a manufacturer-issued, time-limited operator certification that covers the subjects identified above.

- **Consider Other Technologies to Create Safety and Security**: Technology exists to enable secure cryptographic geofences and flight plans, as opposed to more rudimentary software-defined geofences used by most UAS manufacturers today. Technology also exists to enable verified and unchangeable flight logs that work as a secure flight data recorder onboard the unmanned aircraft (UA) as well as to enable authorized rerouting of UAS while leaving a cryptographically-secure paper trail. In the future, this technology will allow law enforcement to essentially "pull over" a rogue UA that is suspected of airspace violations or other potentially criminal activity. Technology exists to enable, not only the secure identification of the UAS, but also separately the trusted identification of the UAS operator and owner. Secure remote identification, combined with other advanced technologies, will support enforcement against rogue UAS and help enable expanded operations in sensitive airspace.

4. Enable Critical Infrastructure Facilities to Prohibit Unauthorized UAS

Rogue UAS present an elevated risk of harm to the critical infrastructure community, which includes traditional critical infrastructure facilities but also sensitive sites such as stadium sporting events, amusement parks, and other mass gatherings of people. For this reason, it is essential that owners and operators of sensitive sites have the ability to prohibit unauthorized UAS operations near and over their facilities, which will assist law enforcement and proprietors of fixed site facilities in identifying friend versus foe.

Section 2209 of the FAA Extension, Safety and Security Act of 2016 (as amended by Section 369 of the FAA Reauthorization Act of 2018) requires the FAA to establish a procedure by which operators or proprietors of fixed site facilities can petition for a designation to prohibit or restrict the operation of UA in close proximity to such facilities. The corresponding Notice of Proposed Rulemaking (NPRM) was supposed to have been published by March 31, 2019, with a final rule being promulgated within 12 months thereafter. The Section 2209 process will greatly enhance UAS security efforts at sensitive fixed sites and should be implemented as soon as possible.

While unauthorized UAS present a threat, critical infrastructure facilities across the U.S. are also using UAS to monitor and assess critical infrastructure, or for other purposes. Like UAS operating in other sensitive environments, such as disaster response efforts in an area covered by a TFR, this co-mingling of "good" and potentially "bad" UAS requires a secure remote identification that can be trusted. Critical infrastructure facility owners and proprietors must have the ability to mandate the use of secure remote identification technology or set other requirements for UAS operators that seek permission to operate in airspace near and around critical infrastructure facilities.

5. Regulations for Expanded UAS Operations Must be Performance-Based and Consider Risk Factors and Benefits to Society Broadly

Regulations for expanded UAS operations must use performance-based standards and risk-based analysis, as opposed to prescriptive standards, to ensure flexibility for this rapidly evolving industry while addressing safety and security concerns. A performance-based standards approach will enable faster deployment of innovative, safety-enhancing UAS technologies that are essential to enabling expanded UAS operations, such as BVLOS flights and flights near airports and other sensitive airspace. Performance-based standards recognize that there are multiple avenues to deliver on safety, and they offer a pathway for industry and regulators to collaborate on new and existing technologies and keep pace with evolving UAS use-cases.

In addition to using performance-based standards, it is also important that regulators consider risk factors and overall benefits to society. In other words, regulators must consider the risks inherent in the dangerous tasks that UAS operations would replace. For example, when considering the risks of flying a UA over an industrial site, the risk analysis should consider the much larger risk of conducting the same inspection using more traditional dangerous methods, such as requiring a human to climb a tower, transmission line, wind turbine or flare stack at a refinery for an inspection. If risk can be appropriately compared, and the use of UAS decreases overall risk, then the UAS application should be readily approved. To this point, the National Academies of Sciences, Engineering, and Medicine has recently issued an influential report urging the federal government to consider risk factors and benefits related to UAS integration more broadly in its decision making.[1]

6. The FAA Must Retain Regulatory Authority on Matters Related to Aviation Safety

It is essential that basic Federalism principles continue to apply to the regulation of airspace, including operation of all aircraft in the NAS. UAS are aircraft subject to regulation by the FAA to ensure safety of flight, and safety of people and property on the ground. While Congress has vested the FAA with the authority to regulate the areas of airspace use, management and efficiency, air traffic control, and aircraft noise at its source, among other areas,[2] states and local jurisdictions are increasingly exploring regulation of UAS or proceeding to enact legislation relating to UAS operations. This has the potential to create a "patchwork quilt" of differing restrictions which is significant because "[s]ubstantial air safety issues are raised when state or local governments attempt to regulate the operation or flight of aircraft."[3] To ensure the maintenance of a safe and sound air transportation system and of navigable airspace free from

[1] See, https://doi.org/10.17226/25143.
[2] *See, e.g.*, 49 U.S.C. §§ 40103, 44502, 44701-44735.

[3] State and Local Regulation of UAS – Fact Sheet (FAA, Office of Chief Counsel, December 17, 2015).

inconsistent restrictions, the FAA must retain regulatory authority over matters pertaining to aviation safety.

One “middle ground” option is for the FAA to provide states and localities the option of implementing one of a few different regulatory operational frameworks, which would vary based on an environment’s risk profile. This “controlled choice” concept would enable the FAA to keep its authority, while granting local jurisdictions the flexibility to enable either an increased economic advantage or heightened airspace safety, without creating a complicated patchwork of paralyzing requirements.

CONCLUSION

UAS technology is already bringing substantial safety and economic benefits to the American people and creative minds will inevitably devise many more UAS uses that will save lives, save money, and make our society more productive.

All technology can be used for good and for bad, and UAS are no different. Recent unauthorized UAS incursions raise unique questions and policy challenges. What is clear, however, is that to enable expanded commercial UAS operations in the U.S., government and UAS industry stakeholders must work together collectively to find a way to integrate UAS into our NAS in a way that is safe and secure. The airspace security concepts addressed in this white paper provide a path forward for doing so.

Expansion of UAS technologies and applications will require secure and ubiquitous remote identification, the availability of effective and integrated counter-UAS systems for critical infrastructure, and federal preemptive authority and guidance to ensure safety and uniformity in the NAS.

A forthcoming paper will address what the policy framework presented here looks like from an operational view.

WHITEFOX

ABOUT WHITEFOX

WhiteFox is a global leader in drone airspace security. Pioneering the safe integration of drones into society, WhiteFox products securely manage drones in sensitive airspace worldwide.

WhiteFox began as a drone manufacturer, but once it became apparent there was no mechanism of enforcement to protect against their misuse, they set out to invent a solution to defend against drone threats. WhiteFox develops products that save lives, protect property, and safeguard privacy.

WhiteFox's mission is to keep the sky open for responsible pilots, advancing drone technology for the benefit of society. In a constantly changing industry, WhiteFox is pushing the boundaries of what security means.

ABOUT LUKE FOX

Luke Fox is Chief Executive Officer at WhiteFox. With extensive technical and operational knowledge in autonomous vehicle technology and security, Luke serves as a subject matter expert (SME) across a number of industry leading advisory groups such as ASTM International, American National Standards Institute (ANSI), Consumer Technology Association (CTA), and FBI InfraGard.

Outside of WhiteFox, Luke is a strong, persistent advocate for children's rights, legislative reform, and is actively involved in the technology community on the central coast of California where he lives and works. Luke was named in Forbes 30 Under 30 for his ongoing innovation and advocacy.

ABOUT DR. RYAN JENKINS

Dr. Ryan Jenkins specializes in applied ethics and consequentialism with focus on robotics and autonomous vehicle technology. Dr. Jenkins serves as Director of Ethics & Policy at WhiteFox and is an assistant professor of philosophy and senior fellow at the Ethics + Emerging Sciences Group at California Polytechnic State University. Dr. Jenkins earned his PhD in Philosophy from the University of Colorado Boulder.