WHITEFOX

March 2, 2020

Submitted Electronically via regulations.gov

The Honorable Elaine L. Chao
Secretary, U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

The Honorable Stephen Dickson
Administrator, Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

Re: Comments of WhiteFox on the Notice of Proposed Rulemaking regarding Remote Identification of Unmanned Aircraft Systems (Docket No. FAA–2019–1100)

Dear Secretary Chao and Administrator Dickson:

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 believes that a comprehensive drone security framework will pave the way for the continued expansion of the commercial drone marketplace, enabling the industry to bring the safety, security, and efficiency benefits of public safety and commercial drones to the American public. WhiteFox has been strongly supportive of the federal government's desire to establish a comprehensive Remote ID framework. WhiteFox has actively participated as part of the ASTM International's Working Group drafting the specification for Remote ID of UAS, and participated in a demonstration of Secure Remote ID in conjunction with the Federal Aviation Administration (FAA) at the International Civil Aviation Organization (ICAO) symposium in November 2019.

WhiteFox works with many government and UAS industry stakeholders. Guided by the benefit of its experience, WhiteFox is pleased to provide formal comments on the FAA's Notice of Proposed Rulemaking (NPRM) on Remote Identification (Remote ID) of UAS.[1]

BACKGROUND

WhiteFox appreciates the federal government's efforts to design a comprehensive Remote ID framework. Remote ID is not only required for safety and security, but it will promote innovation and unlock billions of dollars of economic opportunity.

Indeed, 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 domestic 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 Remote ID framework may have assisted authorities in identifying the rogue UAS operator. As another example, in April of 2019, a rogue UAS was spotted hovering over Boston's Fenway Park during a Major League Baseball game in violation of an FAA Temporary Flight Restriction (TFR). More recently, a man was arrested and charged with violating a TFR after operating his UAS near Hard Rock Stadium in Miami in the week leading up to Super Bowl LIV. Meanwhile, small consumer UAS have been used abroad to deliver weapons.

[1] 84 FR 72438 (December 31, 2019).

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.

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. Remote ID is the critical building block for expanding commercial UAS operations while ensuring airspace security in the U.S., and to that end WhiteFox praises the FAA and other federal agency stakeholders for their efforts to design such a framework. That being said, there are some important changes that the FAA should make to the NPRM before it becomes a Final Rule.

We generally endorse the comments of the Commercial Drone Alliance. We also offer several additional comments on various details of the NPRM's framework here.

1. WhiteFox Supports the Proposed Applicability Thresholds for Remote ID Compliance

In order to protect against potential public safety and security threats posed by rogue UAS, it is essential that the NPRM require nearly all UAS operating in the National Airspace System (NAS) to comply with Remote ID. For this reason, WhiteFox supports the NPRM's proposal to tie compliance with Remote ID to registration under part 47 or part 48 of the Federal Aviation Regulations (FARs) and to the operation of foreign civil UAS in the U.S.[2] With limited exceptions, this will require nearly all UAS weighing 250 grams or more to comply with Remote ID. Including UAS weighing 250 grams or more is comprehensive, encompassing the majority of UAS except for very small and unsophisticated UAS. The weight threshold also aligns with and builds upon existing UAS registration requirements, and supports robust UAS traffic management (UTM) systems.

Notably, future advancements in UAS technology may necessitate that the Remote ID applicability requirements be expanded to cover a broader set of UAS, including UAS weighing

[2] *Id.* at 72461.

less than 250 grams.

2. Performance-Based Requirements Will Help Future-Proof Remote ID

WhiteFox agrees with the NPRM's adoption of a regulatory framework with flexible performance-based requirements, rather than prescriptive requirements which could likely become outdated in a few short months or years. As proposed in the NPRM, a person submitting a means of compliance would be able to develop their own means to meet Remote ID objectives and goals.[3] The flexibility to develop a means of compliance, which could include consensus standards, will allow the Remote ID regulatory framework to keep pace with rapid advancements in UAS technology and will provide stakeholders with the flexibility to innovate on different pathways to meeting the underlying safety and security objectives of Remote ID.

3. A "Secure" Remote Identification Category Should be Incorporated into the NPRM

The NPRM proposes a tiered approach for Remote ID, and as a general matter WhiteFox believes this is appropriate. However, the NPRM should be revised to incorporate an additional tier for a trusted Secure Remote ID. As proposed, both Limited and Standard Remote ID UAS would be required to transmit Remote ID information that is not encrypted and is accessible to anyone. Absent proper security protections, UAS identities can be easily impersonated, forged, or modified without detection at little to no cost. In its current form, the FAA's proposal lacks the security elements necessary to trust the Remote ID information being transmitted, and without trust there cannot be accountability. For certain low risk and simple operations, within visual line of sight in unpopulated areas for example, an easy to incorporate Remote ID standard is most appropriate. However, a higher-security Remote ID solution must be adopted for UAS operating in and around our nation's most sensitive airspace and for more complex expanded UAS operations, like BVLOS operations.

With Secure Remote ID, the need to exempt certain operators (such as law enforcement or federal agencies) from Remote ID requirements would also be minimized or eliminated.[4] Excluding certain classes of operators is counterintuitive to the goal of establishing a universal and comprehensive Remote ID framework, and this is not the answer. Rather, operators with an

[3] *Id.* at 72472.

[4] Proposed § 89.110(a), Standard remote identification of unmanned aircraft systems, is prefaced with "[u]nless otherwise authorized by the Administrator", which infers that some operators may be authorized by the FAA not to comply with remote identification operating requirements. *Id.* at 72517.

enhanced need for privacy and authentication should be required to use Secure Remote ID. With Secure Remote ID it would be possible to obscure sensitive information for certain operations that require enhanced privacy protections. For example, depending on the nature of the UAS operation, law enforcement entities operating UAS may need to shield certain information from the general public. Mandating Secure Remote ID for these operations would allow law enforcement to comply with Remote ID, while at the same time providing them with enhanced privacy protections that may be necessary depending on the unique nature of the mission being performed.

Finally, while Secure Remote ID should be mandatory for certain operators, the ability to use Secure Remote ID should be available to all operators. For example, certain commercial UAS operators have expressed concern with people exploiting the open nature of Standard Remote ID for potential theft of proprietary information or other malicious activity. There should be a mechanism for these commercial operators to opt into a Known Operator Program that provides the benefit of Secure Remote ID, including extra privacy protections.

Secure Remote ID may be especially beneficial for sensitive facilities. Indeed, rogue UAS present an elevated risk of harm to critical infrastructure facilities and other sensitive sites such as stadium sporting events, amusement parks, and other mass gatherings of people. Proprietors of these sensitive sites must have the ability to mandate Secure Remote ID technology for operators that seek to operate near and around their facilities. Absent the ability to mandate Secure Remote ID, it will be impossible for proprietors of these sensitive facilities to differentiate between authorized and unauthorized UAS operations because Remote ID that lacks necessary cybersecurity protections is susceptible to forgery and cannot be trusted.

4. Allow for Retrofitting of Legacy and New UAS Using Retrofit Modules

While the proposed rule contemplates the ability of UAS manufacturers to retrofit existing legacy UAS to comply with Remote ID requirements through software or "push" updates,[5] not all existing UAS have the necessary Remote ID hardware capability that would enable retrofitting via software updates from the UAS manufacturer. In its current form, the NPRM would make all UAS that cannot be retrofitted via a software update from the manufacturer illegal to operate anywhere outside of a FAA-recognized identification area (FRIA) once the rule takes full effect. The economic impact on commercial operators operating this category of

[5] *Id.* at 72489.

legacy UAS will be substantial because the UAS will essentially become useless from a commercial-use perspective.

The NPRM states that FAA is relying on industry research showing that 93% of the current Part 107 fleet of UAS would be capable of receiving a software update retrofit from the OEM. This cannot be known prior to a Means of Compliance and operational testing. Further, simply expecting UAS to "expire" is not consistent with the fact that there are older drones that are frequently used for commercial operations today. For example, DJI Phantom 2 UASs are still commonly used today even though they were released in 2013, nearly seven years ago.

The NPRM should be revised to allow for UAS to be retrofitted with Remote ID modules manufactured by third-parties other than the UAS OEM. Authorizing compliance through retrofit modules for legacy and new UAS by third-parties will allow for an expedited Remote ID implementation timeline and support domestic UAS manufacturers by decreasing barriers to market entry.

Indeed, technology currently exists that would allow a UAS that is otherwise not capable of being retrofitted by the UAS manufacturer to be retrofitted by a Remote ID module from a third party. For example, by enabling compliance with the Remote ID requirements vis-a-vis retrofit modules, the NPRM would reduce costs to operators and barriers to entry associated with the loss of UAS use that would otherwise occur if the operator is unable to easily retrofit the UAS for compliance with Remote ID requirements.

Beyond retrofits of existing legacy UAS, the NPRM should also be revised to allow newly manufactured UAS to comply with Remote ID requirements via retrofit using modules. Rather than placing stringent production requirements solely for the UAS manufacturer, the NPRM should allow for those same obligations to be assumed by a retrofit module manufacturer. Enabling the use of retrofit modules would allow for quicker and less expensive means of implementing a comprehensive Remote ID framework. A UAS Module Retrofit Manufacturer category should be created to enable industry to submit a Means of Compliance. Allowing for the use of retrofit modules would also decrease barriers to market entry for U.S. domestic UAS manufacturers because stringent design and production requirements could be assumed by a specialized domestic retrofit module manufacturer.

5. With Limited Exceptions, All UAS Should be Standard Remote ID UAS

In order to achieve the NPRM's public safety and security goals, the vast majority of UAS operating in the NAS should be Standard Remote ID UAS. In order for law enforcement to mitigate threats caused by rogue UAS, law enforcement must be able to distinguish "good" from "bad" UAS, or friend from foe (IFF). WhiteFox agrees with the NPRM's requirement for Standard Remote ID to both transmit Remote ID information to a USS via network and broadcast Remote ID information, however, WhiteFox disagrees with the proposal to prohibit Limited Remote ID UAS from broadcasting Remote ID. While only transmitting Remote ID information via network to a USS may be sufficient in some scenarios and locations, to ensure that law enforcement are able to distinguish authorized from unauthorized UAS operations, all UAS should generally be required to broadcast Remote ID information as well.

The default requirement should be Standard Remote ID, however WhiteFox does agree with the NPRM's proposal to exclude a small category of UAS operated within the boundaries of an FAA-recognized identification area and for the exclusion of UAS operated for the purpose of aeronautical research or to show compliance with regulations.[6]

In its current form, the NPRM would require that Limited Remote ID UAS only transmit an indication of the latitude and longitude of the control station and not the location of the UA itself.[7] In an environment where both authorized and unauthorized UAS may be operating simultaneously, law enforcement must be able to identify which specific UA(s) poses a threat. In order to make this determination, law enforcement must be able to remotely identify the UA itself, not just the ground control station. The NPRM should be revised to mandate that all UAS that are required to comply with Remote ID transmit the location of the UA; otherwise it defeats the entire purpose of establishing a comprehensive and universal Remote ID framework.

Finally, since requiring Limited Remote ID UAS to broadcast and transmit the location of the UA would essentially eliminate any meaningful distinction between Standard and Limited Remote ID UAS, WhiteFox believes that the FAA should eliminate the Limited category of Remote ID UAS. In order for Remote ID to be successful, universal participation is necessary. By not requiring Limited Remote ID UAS to broadcast Remote ID, including the location of the UA itself, the NPRM significantly undermines the safety and security goals of establishing a

[6] *Id.* at 72466-67.
[7] *Id.* at 72446.

Remote ID framework. Moreover, the Limited Remote ID category is not necessary because, as discussed above, Limited Remote ID UAS could be retrofitted with a module from a retrofit manufacturer which is capable of converting a Limited Remote ID UAS into a Standard Remote ID UAS.

6. The Final Rule Must Clarify Remote ID Cybersecurity Requirements

The NPRM requires that Standard and Limited Remote ID UAS incorporate cybersecurity protections for the transmission and broadcast of Remote ID message elements, as appropriate.[8] The FAA, however, goes on to note that it is not proposing any specific cybersecurity protection methods and that cybersecurity would be evaluated in the context of reviewing a proposed FAA-accepted means of compliance (MOC).[9] While it may be appropriate to defer specific methods to the MOC review, the rule should, at the very least, clarify the minimum performance standards for cybersecurity. To that end, the rule should clarify how the MOC for cybersecurity will be evaluated. Cybersecurity should be defined as providing a means of ensuring confidentiality, integrity/authenticity (anti-spoofing/tampering), authorization/access control, freshness, and validation of Remote ID messages with different levels required for Standard and Secure Remote ID.

Cybersecurity must also be considered when qualifying UAS Service Suppliers (USS). Under the NPRM, both Standard and Limited Remote ID UAS would be required to transmit Remote ID information to a USS via a network connection.[10] As part of the USS qualification process, the NPRM states that "[p]rospective Remote ID USS would also be reviewed for consistency with national security and cybersecurity requirements and export administration regulations." WhiteFox strongly supports a requirement for the FAA to consider U.S. national security and cybersecurity requirements and export administration regulations when vetting a potential USS. A Remote ID USS will have access to a wealth of sensitive information and data that is not otherwise available to the public and could be used to, among other things, invade privacy and steal intellectual property and other sensitive data.

The NPRM also states that the "FAA anticipates that some UAS manufacturers will also be Remote ID USS."[11] It is WhiteFox's position that allowing UAS OEMs to serve as a Remote ID USS for its own products should not be permissible under the Remote ID rule because it allows

[8] *Id.* at 72478.
[9] *Id.*
[10] *Id.* at 72484.

for consolidation of hardware and infrastructure, which creates compromised risk.

7. The FAA Should Provide Incentives to Encourage Early Voluntary Remote Identification

Consistent with the recommendations of the Remote Identification Incentives Subgroup of the Drone Advisory Committee (DAC)[12], the FAA should provide operators with incentives immediately after the rulemaking process is complete to encourage early adoption of Remote ID prior to the Remote ID rule taking effect. These incentives should include, among other things: (1) prioritizing waiver applications for operators who have Remote ID; (2) giving government contract preference to operators who have Remote ID; and (3) considering Remote ID compliance as part of an applicant's safety case to support expanded UAS operations, like night flights, BVLOS flights, and flights over people.

8. UAS Should Be Required to Broadcast Message Elements Using Openly Published Protocol

The NPRM proposes in § 89.310(i)(2) to "require that standard remote identification UAS be capable of broadcasting the message elements in proposed § 89.305 using a non-proprietary broadcast specification and radio frequency spectrum in accordance with 47 CFR part 15 that is compatible with personal wireless devices."[13] As of today, most commercially available cell phones are not capable of receiving such broadcasts, and therefore the Remote ID rule should not require that the broadcast message be receivable by most personal wireless devices (i.e., the broadcast requirement should not be tied to a technology that does not currently exist). The ASTM F38 Remote ID working group spent over a year evaluating potential broadcast solutions. The results are as follows: Bluetooth 4 has very limited range (50 meters). Bluetooth 5 has natively slightly longer range than Bluetooth 4, however the optional long-range capability requires specific chipsets that are rarely used. For example, most phones such as new iPhones do not have appropriate chipsets for the long-range capability. As for WiFi, the two leading methods are SSID Stuffing and WiFi-Aware. SSID Stuffing floods the WiFi channels creating interference for WiFi users and gibberish for the general public looking at available WiFi networks, and is incompatible with iPhones (about 40% of U.S. cell phones) due to security

[11] *Id.*
[12] https://www.faa.gov/uas/programs_partnerships/drone_advisory_committee/media/eBook_10-17-2019_DAC_Meeting.pdf,
[13] 84 FR at 72476.

implications. WiFi-Aware is the method included in the ASTM standard. It is only available on a small number of phone models (about three known) with no certainty it will ever meet the threshold of "commonly available." Instead, the Remote ID rule should simply require that the message elements be broadcasted over non-proprietary ISM bands.

9. A Three-Year Implementation Period is Unnecessarily Long

Under the NPRM, with limited exceptions, UAS operating in the NAS would not need to comply with Remote ID requirements until three years after the effective date of the rule.[14] The implementation of a comprehensive Remote ID system is essential to establishing reasonable controls to protect against potential safety and security threats posed by UAS. In addition to addressing safety and security needs, a Remote ID framework is a foundational building block to enabling expanded operations beyond Part 107, including, but not limited to, operations over people and BVLOS operations, as well as the development of UTM. A three-year Remote ID implementation timeline is unnecessarily long and will have a devastating effect on the ability to further integrate UAS into the NAS for years to come. As discussed above, modifications to aspects of the NPRM relating to retrofit modules for existing UAS on the market would make it simpler and less costly to comply with Remote ID requirements and would support a shorter timeframe for implementation of Remote ID requirements.

CONCLUSION

WhiteFox commends the FAA for taking another step to integrate UAS safely and securely into the national airspace and generally supports the proposed rules with some modifications as discussed above.

Respectfully submitted,

WhiteFox Defense Technologies, Inc.

By: *Luke Fox*

Luke Fox
Chief Executive Officer
833 Buckley Road, San Luis Obispo, CA
(805) 250-9690

[14] *Id.* at 72439.