

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AXON ENTERPRISE, INC. AND DEDRONE HOLDINGS, INC.
Petitioners

v.

AIRSPACE DEFENSE, INC.
Patent Owner

Case No. IPR2025-00530
Patent 10,249,199

**PETITIONERS' SUBMISSION REGARDING THE AUGUST 27, 2026
ORDER (PAPER 42)**

Pursuant to the Board's Order (Paper 42) dated August 27, 2026 regarding *Dental Monitoring SAS v. Align Tech.*, 2026 WL 2291181 (Fed. Cir. Aug. 10, 2026), Petitioners submit herewith claim charts for U.S. Patent Application Publication No. 2019/0003807 to Whitmarsh (EX1005) ("Whitmarsh") and U.S. Patent No. 9,805,238 to Falk (EX1011) ("Falk").

With respect to Whitmarsh (EX1005), the enclosed chart of Appendix A demonstrates that claim 19 of Whitmarsh is supported by U.S. Provisional Application No. 62/267,393 (EX1006) (the "'393 Provisional") filed December 15, 2015. The Petition (Paper 13) and Opposition (Paper 32) demonstrated where the specific subject matter relied on in Whitmarsh was supported by the '393 Provisional. *See, e.g.* Petition, 15-51 (analysis including citations to Whitmarsh (EX1005) and parallel citations to the '393 Provisional (EX1006)); Opposition, 6-25 (same). Whitmarsh thus qualifies as prior art to U.S. Patent No. 10,249,199 (the "'199 Patent") under 35 U.S.C. § 102(a)(2) as of the December 15, 2015 filing date of the '393 Provisional. *See* Opposition, 6-7; Petition, 5.

With respect to Falk (EX1011), the enclosed chart of Appendix B demonstrates that claim 1 of Falk is supported by U.S. Provisional Application No. 62/301,858 (EX1012) (the "'858 Provisional") filed March 1, 2016. The Petition and Opposition demonstrated where the specific subject matter relied on in Falk was supported by the '858 Provisional. *See, e.g.*, Petition, 35-40, 51, 69-73 (analysis

including citations to Falk (EX1011) and parallel citations to the '858 Provisional (EX1012)); Opposition, 19, 25. Falk thus qualifies as prior art to the '199 Patent under 35 U.S.C. § 102(a)(2) as of the March 1, 2016 filing date of the '858 Provisional. *See* Opposition, 6-7; Petition, 5.

Respectfully submitted,

BAKER BOTTS L.L.P.

A handwritten signature in black ink, appearing to read "Chad C. Walters", written in a cursive style.

Chad C. Walters (Reg. No. 48,022)
Lead Counsel for Petitioners

Date: September 1, 2026

APPENDIX A

Whitmarsh (EX1005), Claim 19	U.S. Provisional Application No. 62/267,393 filed December 15, 2015 (EX1006) (the “’393 Provisional”)¹
[19a] A method of defending against an unmanned aerial vehicle, comprising:	The ’393 Provisional discloses using systems for defending against unauthorized incursions by an unmanned aerial vehicle and thus supports <i>[a] method of defending against an unmanned aerial vehicle</i> as claimed. “The present invention relates to defense systems in general and more particularly to systems for defending against unauthorized incursions by unmanned aerial vehicles.” EX1006, ¶0001. “Various embodiments of a drone defense system (DDS) are shown and described herein as they could be used to effect one or more countermeasures against unwanted or unauthorized drone incursions into defined air space. Additional information regarding the present invention is contained in Attachment A, which is attached hereto and forms a part of the disclosure.” EX1006, ¶0003. “The drone defense system is capable of countering, mitigating and/or interdicting of unmanned aerial systems and unmanned aerial vehicles. The drone defense system may also involve a remote transmission security system (RTSS) which may be used to take control of or commandeer an unauthorized, undesired, or rogue drone to the point of returning it back to the sender while capturing and recording its location and if the rogue drone is equipped with a camera, take a photo of the rogue drone operator's face or any other physical ID. The RTSS process can include other forms of response. One example is having an armed security drone automatically respond to the tagged drones that have trespassed in a secure area as an extra countermeasure, in addition to documenting the location of origin where

¹ Bolding contained in the quoted portions is emphasis added.

	the rogue drone was launched. The DDS has several countermeasure behaviors that can be programmed into to the Remote Transmission Security System, which allows for further customization.” EX1006, ¶0006. “Drone Defense Systems improves on any system by defending against Rogue Drones, by implementing an ability to ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses....” EX1006, page 23.
[19b] monitoring a sensing area for the presence of the unmanned aerial vehicle;	The '393 Provisional discloses that use of its systems includes monitoring a protected area/region, as well as areas within a 10-mile, 5-mile, and 1-mile radius of the protected area/region, for the presence of the unmanned aerial vehicle based on sensed signals from the unmanned arial vehicle. This process determines whether the unmanned aerial vehicle is present in the protected area/region and areas within the 10-mile, 5-mile, and 1-mile radiuses and if it is a threat, and supports <i>monitoring a sensing area for the presence of the unmanned aerial vehicle</i> as claimed. “The drone defense system is capable of countering, mitigating and/or interdicting of unmanned aerial systems and unmanned aerial vehicles. The drone defense system may also involve a remote transmission security system (RTSS) which may be used to take control of or commandeer an unauthorized, undesired, or rogue drone to the point of returning it back to the sender while capturing and recording its location and if the rogue drone is equipped with a camera, take a photo of the rogue drone operator's face or any other physical ID. The RTSS process can include other forms of response. One example is having an armed security drone automatically respond to the tagged drones that have trespassed in a secure area as an extra countermeasure, in addition to documenting the location of origin where the rogue drone was launched. The DDS has several countermeasure behaviors that can be programmed into to the Remote

Transmission Security System, which allows for further customization.” EX1006, ¶0006.

“The RTSS operates in conjunction with one or more ‘smart’ devices comprising the drone defense system, such as, for example, sonar/radar sensors and applications that work with other components, including highly specialized classified security firmware and classified security software. **RTSS is the first defensive system that can ID a drone's signature.** When all parts are connected and applied, a logic control response is activated to keep the property secure and safe.” EX1006, ¶0007.

“The RTSS constantly analyzes all of the parameters of the network that it is monitoring and it continuously processes all information from different UAS or drone signatures that are hostile and non-hostile that come within a 10-mile, 5-mile, and 1-mile area of a defined airspace system that is to be protected. The RTSS is thus an important aspect of the drone defense system: **The RTSS creates a virtual ‘dome’ to protect the defined airspace that is to be protected.**” EX1006, ¶0008.

“The primary function of the RTSS is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone.” EX1006, ¶0009.

“In some embodiments, a general operational environment and/or parameters for the drone defense system (DDS) may be as follows:

- 1) The DDS will be able to determine between friendly and hostile drones.
- 2) **DDS coverage includes three-dimensional (e.g., X,Y,Z axis) coordinates in an automated system that covers Z**

space from ground level to 20,000 feet and X space of maximum 10 miles and Y space by 10 miles maximum.

3) DDS logic environment covers all type of behaviors, such as velocities from 1 to 100+ meters/second (m/s).

4) DDS does not rely on size to determine the ID of hostile drones and tag them. It focuses on the drone speed zone of 87.0 knots (100 mph) max.

5) DDS does not rely on material compositions of the hostile drones to ID and tag them.

6) DDS identification, tracking, tagging, and countermeasures functions may be configured to cover or apply to all drones regardless of whether they are commercial models or custom made. All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS and used to identify the drone.

7) **DDS may be configured to track, tag, and engage countermeasures that can go as far out as 10 miles, 5 miles, or 1 mile with a kill zone in each segment.**

8) **DDS uses many elements that track GPS of all drones.”**

EX1006, ¶0013.

“In one embodiment, **the DDS consists of an electronic remote monitoring device**, a classified firmware, different antennas from wireless to satellite depending on what the facilities require and **the required area coverage**, and a classified software that has an interactive GUI which can communicate with any device and any Internet-enabled (IoT) system.” EX1006, ¶0014.

“In some embodiments, **the DDS constantly scans and surveys WIFI, RF, and sensor signals and processing** an auto- logic: An 'if-then' logic may be used to determine different solutions in relationship to the threat.” EX1006, ¶0015.

“The **DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with**

	definable MAC addresses are tagged by the DDS. All non-MAC address drones activate the countermeasures system.” EX1006, ¶0016. “DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry. In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as ‘friendly’ or ‘authorized’ will allowed to travel from x miles marks to point zero.” EX1006, ¶0017.
[19c] detecting a radio signal broadcast by the unmanned aerial vehicle;	The ’393 Provisional discloses that use of its systems includes detecting RF signals broadcast by the unmanned aerial vehicle and thus supports <i>detecting a radio signal broadcast by the unmanned aerial vehicle</i> as claimed. “The RTSS constantly analyzes all of the parameters of the network that it is monitoring and it continuously processes all information from different UAS or drone signatures that are hostile and non-hostile that come within a 10-mile, 5-mile, and 1-mile area of a defined airspace system that is to be protected. The RTSS is thus an important aspect of the drone defense system: The RTSS creates a virtual ‘dome’ to protect the defined airspace that is to be protected.” EX1006, ¶0008. “The primary function of the RTSS is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone.” EX1006, ¶0009.

“In one embodiment, **the DDS consists of an electronic remote monitoring device, a classified firmware, different antennas from wireless to satellite depending on what the facilities require and the required area coverage**, and a classified software that has an interactive GUI which can communicate with any device and any Internet-enabled (IoT) system. It will function on a Wi-Fi network, so the DSS may interface with a secure network. Antennae may be positioned unobtrusively throughout a facility to provide full communications coverage. The DDS may be configured to communicate via a secure, encrypted Internet cloud-enabled connection to local and national databases, a facility security system, and law enforcement entities. DDS is highly adaptive. The DDS system can be configured on an available facility's infrastructure. The DDS can be customized for specific needs of a particular user.” EX1006, ¶0014.

“In some embodiments, **the DDS constantly scans and surveys WIFI, RF, and sensor signals and processing an auto- logic: An 'if-then' logic may be used to determine different solutions in relationship to the threat.**” EX1006, ¶0015.

“**The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with definable MAC addresses are tagged by the DDS. All non-MAC address drones activate the countermeasures system.**” EX1006, ¶0016.

“**DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry.** In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the

	countermeasure system. Only drones registered on the local registry as 'friendly' or 'authorized' will allowed to travel from x miles marks to point zero." EX1006, ¶0017. "Drone Defense System (DDS) answers the growing number of drones that have been flown dangerously close to commercial aircraft and other rogue Drone activities that violate federal rules for their operation. The DDS Remote Transmission Security Systems (RTSS), code named, 'Return to Sender', Detects, Records, Tracks, Targets, Counter Measures, Tags and Intercepts/Control the Rouge drone from 10 meters to 100,000 meters from the threatened object. Different type of countermeasures will be deploy according to the rule of engagement pertaining to the specific DDS Model." EX1006, page 22. "Drone Defense Systems improves on any system by defending against Rogue Drones, by implementing an ability to ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses...." EX1006, page 23.
[19d] identifying the unmanned aerial vehicle;	The '393 Provisional discloses that use of its systems includes identifying the unmanned aerial vehicle, such as by its media access control (MAC) address, and thus supports <i>identifying the unmanned aerial vehicle</i> as claimed. "The primary function of the RTSS is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone." EX1006, ¶0009. "The first process for RTSS after detection is tracking and analyzing all signatures of the different devices, elements, and components within protected zones. RTSS

determines threat level and identifies (IDs) the drones. In one embodiment, the RTSS identifies, classifies, and categorizes the unauthorized or hostile drones by their signatures. Each movement is computed and observed. Each tracking signature may be processed in conjunction with one or more information databases, including, for example a local database or a national database (the national registry database structure is currently being defined) to record the signature of each non-recognized signature and each event. **The RTSS will record them and once the national database is online, it will attempt to match the signature of the drone or device with its owner. The behavior of the unauthorized or hostile drone is recorded with its signature identification. If the tracking signature matches a rule in the logic system that the unauthorized or hostile drone's identification signatures are a threat, the RTSS 'tags' the drone as unauthorized or even as hostile. Immediately, a series of processes are started to determine what rule of engagement will be applied on the intruding drone. The engagement responses are determined by the behavior of the hostile drone and other instructions. If there is a threat, the system will take the next step to response.** These actions occur in milliseconds from the feeds of the apparatus; there are constant communications with the internal (local) and national databases.” EX1006, ¶0010.

“6) DDS identification, tracking, tagging, and countermeasures functions may be configured to cover or apply to all drones regardless of whether they are commercial models or custom made. All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS and used to identify the drone.” EX1006, ¶0013.

“The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with definable MAC addresses are tagged by the DDS. All

non-MAC address drones activate the countermeasures system.” EX1006, ¶0016.

“DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry. In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as ‘friendly’ or ‘authorized’ will allowed to travel from x miles marks to point zero.” EX1006, ¶0017.

“Drone Defense System (DDS) answers the growing number of drones that have been flown dangerously close to commercial aircraft and other rogue Drone activities that violate federal rules for their operation. The DDS Remote Transmission Security Systems (RTSS), code named, ‘Return to Sender’, Detects, Records, Tracks, Targets, Counter Measures, Tags and Intercepts/Control the Rouge drone from 10 meters to 100,000 meters from the threatened object. Different type of countermeasures will be deploy according to the rule of engagement pertaining to the specific DDS Model.” EX1006, page 22.

“Drone Defense Systems improves on any system by defending against Rogue Drones, by implementing an ability to ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses....” EX1006, page 23.

[19e] developing a countermeasure based on the identity of the unmanned aerial vehicle; and	The '393 Provisional discloses that use of its systems includes identifying the unmanned aerial vehicle by its MAC address and determining that the MAC address is not registered with a registry, which means the unmanned aerial vehicle is considered a threat. A series of processes then occurs to determine a rule of engagement and engagement response—which includes various countermeasures—applied to the unmanned aerial vehicle that is a threat. One engagement response is a “commandeer” countermeasure, in which the remote transmission security system (RTSS) takes over control of the unmanned aerial vehicle and forces it to land. Another engagement response is a “drone destruct” countermeasure, in which the RTSS takes over control of the unmanned aerial vehicle and causes it to self-destruct or otherwise become inoperable. This thus supports <i>developing a countermeasure based on the identity of the unmanned aerial vehicle</i> as claimed. “The drone defense system is capable of countering, mitigating and/or interdicting of unmanned aerial systems and unmanned aerial vehicles.” EX1006, ¶0006. “The primary function of the RTSS is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone.” EX1006, ¶0009. “The first process for RTSS after detection is tracking and analyzing all signatures of the different devices, elements, and components within protected zones. RTSS determines threat level and identifies (IDs) the drones. In one embodiment, the RTSS identifies, classifies, and categorizes the unauthorized or hostile drones by their signatures. Each movement is computed and observed. Each tracking signature may be processed in conjunction
---	--

with one or more information databases, including, for example a local database or a national database (the national registry database structure is currently being defined) to record the signature of each non-recognized signature and each event. **The RTSS will record them and once the national database is online, it will attempt to match the signature of the drone or device with its owner. The behavior of the unauthorized or hostile drone is recorded with its signature identification. If the tracking signature matches a rule in the logic system that the unauthorized or hostile drone's identification signatures are a threat, the RTSS 'tags' the drone as unauthorized or even as hostile. Immediately, a series of processes are started to determine what rule of engagement will be applied on the intruding drone. The engagement responses are determined by the behavior of the hostile drone and other instructions. If there is a threat, the system will take the next step to response. These actions occur in milliseconds from the feeds of the apparatus; there are constant communications with the internal (local) and national databases.**" EX1006, ¶0010.

"The response engagement will determine what type of countermeasure would occur and at what distance. Exemplary countermeasures that may be applied or executed by the drone defense system include, but are not limited to, the following countermeasures:...3) **Commandeer.** In this countermeasure, the RTSS actually takes over control of the hostile or unauthorized drone, forcing it to land away from the protected area. Law enforcement agencies (e.g., local law enforcement, the FBI, the DHS, etc) may then be notified and appropriate action taken. 4) **Drone Destruct.** In this countermeasure, the RTSS also takes over control or commandeers the hostile or unauthorized drone and may cause it to self-destruct or otherwise become inoperable (e.g., by initiating a power overload in the drone's power supply system)." EX1006, ¶0011.

“6) DDS identification, tracking, tagging, and countermeasures functions may be configured to cover or apply to all drones regardless of whether they are commercial models or custom made. All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS and used to identify the drone.” EX1006, ¶0013.

“The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with definable MAC addresses are tagged by the DDS. All non-MAC address drones activate the countermeasures system.” EX1006, ¶0016.

“DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry. In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as ‘friendly’ or ‘authorized’ will allowed to travel from x miles marks to point zero.” EX1006, ¶0017.

“In some embodiments, the countermeasures system is activated under the following conditions or scenarios: 1) Rogue drones are processed by a auto-logic ‘if/then’ logical process which defines, tracks, and tags a drone as hostile or friendly. Activation may occur when the auto-logic intellectual format is triggered by the drone that is hostile or a ‘friendly’ or ‘authorized’ drone that has turned hostile. 2) Drones are considered unauthorized or hostile if they have no registration from their MAC addresses. 3) Drones are considered hostile and activate the countermeasures system if they have a MAC address but it's not registered with the local registry or no MAC

address and has crossed the 5 mile safe zone. 4) **The DDS countermeasure system may be embodied in firmware with firewall systems.** The countermeasure system may also involve a **custom AES algorithm, 256 key length that deploys different types of defenses in destroying the drone vehicle, interrupting flight, controlling flight, returning to the user/sender of the drone for apprehension,** and submitting an electronic record for results for the infractions.” EX1006, ¶0018.

“Drone Defense System (DDS) answers the growing number of drones that have been flown dangerously close to commercial aircraft and other rogue Drone activities that violate federal rules for their operation. **The DDS Remote Transmission Security Systems (RTSS), code named, 'Return to Sender', Detects, Records, Tracks, Targets, Counter Measures, Tags and Intercepts/Control the Rouge drone from 10 meters to 100,000 meters from the threatened object. Different type of countermeasures will be deploy according to the rule of engagement pertaining to the specific DDS Model.**” EX1006, page 22.

“DDS through "RTSS" will apply countermeasures to destroy or control the weaponized drone by returning the Rogue Drone back to the sender and controller, recording and using the Drones resources to ID the owners and destroy or capture the rogue pilot. If there is no GPS return•home behavior activated, **the drone will be forced to land, it will be Electronic or RF jammed and disarmed in flight.** DDS will be intricately integrated with Law Enforcement entities. and Military/National Guard.” EX1006, page 23.

“**Drone Defense Systems** improves on any system by **defending against Rogue Drones,** by implement an ability to **ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses and according to the rules of engagement (these rules can be customized for any protected area) it creates a**

	countermeasure that will disarm, intercept, Return to Sender, or force land a rogue drone.” EX1006, page 23.
[19f] transmitting the developed countermeasure to the unmanned aerial vehicle, the unmanned aerial vehicle subsequently operating in accordance with the developed countermeasure.	The '393 Provisional discloses that use of its systems includes transmitting the “commandeer” countermeasure to the unmanned aerial vehicle, which causes the RTSS to take over control of the unmanned aerial vehicle and force the unmanned aerial vehicle to operate so that it lands. The '393 Provisional also discloses that use of its systems includes transmitting the “drone destruct” countermeasure to the unmanned aerial vehicle, which causes the RTSS to take over control of the unmanned aerial vehicle and cause the unmanned aerial vehicle to operate so that its power supply system experiences a power overload; this overload results in the unmanned aerial vehicle self-destructing or otherwise becoming inoperable. Each of these examples supports <i>transmitting the developed countermeasure to the unmanned aerial vehicle, the unmanned aerial vehicle subsequently operating in accordance with the developed countermeasure</i> as claimed. “The drone defense system is capable of countering, mitigating and/or interdicting of unmanned aerial systems and unmanned aerial vehicles.” EX1006, ¶0006. “The primary function of the RTSS is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone.” EX1006, ¶0009. “The first process for RTSS after detection is tracking and analyzing all signatures of the different devices, elements, and components within protected zones. RTSS determines threat level and identifies (IDs) the drones. In one embodiment, the RTSS identifies, classifies, and

categorizes the unauthorized or hostile drones by their signatures. Each movement is computed and observed. Each tracking signature may be processed in conjunction with one or more information databases, including, for example a local database or a national database (the national registry database structure is currently being defined) to record the signature of each non-recognized signature and each event. **The RTSS will record them and once the national database is online, it will attempt to match the signature of the drone or device with its owner. The behavior of the unauthorized or hostile drone is recorded with its signature identification.** If the tracking signature matches a rule in the logic system that the unauthorized or hostile drone's identification signatures are a threat, the RTSS 'tags' the drone as unauthorized or even as hostile. Immediately, a series of processes are started to determine what rule of engagement will be applied on the intruding drone. The engagement responses are determined by the behavior of the hostile drone and other instructions. If there is a threat, the system will take the next step to response. These actions occur in milliseconds from the feeds of the apparatus; there are constant communications with the internal (local) and national databases." EX1006, ¶0010.

"The response engagement will determine what type of countermeasure would occur and at what distance. Exemplary countermeasures that may be applied or executed by the drone defense system include, but are not limited to, the following countermeasures:...3) **Commandeer.** In this countermeasure, the RTSS actually takes over control of the hostile or unauthorized drone, forcing it to land away from the protected area. Law enforcement agencies (e.g., local law enforcement, the FBI, the DHS, etc) may then be notified and appropriate action taken. 4) **Drone Destruct.** In this countermeasure, the RTSS also takes over control or commandeers the hostile or unauthorized drone and may cause it to self-destruct or otherwise become inoperable (e.g., by initiating a

power overload in the drone's power supply system)."
EX1006, ¶0011.

"The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with definable MAC addresses are tagged by the DDS. All non-MAC address drones activate the countermeasures system." EX1006, ¶0016.

"DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry. In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as 'friendly' or 'authorized' will allowed to travel from x miles marks to point zero."
EX1006, ¶0017.

"In some embodiments, the countermeasures system is activated under the following conditions or scenarios:...2) Drones are considered unauthorized or hostile if they have no registration from their MAC addresses. 3) Drones are considered hostile and activate the countermeasures system if they have a MAC address but it's not registered with the local registry or no MAC address and has crossed the 5 mile safe zone. 4) The DDS countermeasure system may be embodied in firmware with firewall systems. The countermeasure system may also involve a custom AES algorithm, 256 key length that deploys different types of defenses in destroying the drone vehicle, interrupting flight, controlling flight, returning to the user/sender of the drone for apprehension, and submitting an electronic record for results for the infractions." EX1006, ¶0018.

“Drone Defense System (DDS) answers the growing number of drones that have been flown dangerously close to commercial aircraft and other rogue Drone activities that violate federal rules for their operation. **The DDS Remote Transmission Security Systems (RTSS), code named, 'Return to Sender', Detects, Records, Tracks, Targets, Counter Measures, Tags and Intercepts/Control the Rouge drone from 10 meters to 100,000 meters from the threatened object. Different type of countermeasures will be deploy according to the rule of engagement pertaining to the specific DDS Model.**” EX1006, page 22.

“**DDS through "RTSS" will apply countermeasures to destroy or control the weaponized drone by returning the Rogue Drone back to the sender and controller, recording and using the Drones resources to ID the owners and destroy or capture the rogue pilot. If there is no GPS return•home behavior activated, the drone will be forced to land, it will be Electronic or RF jammed and disarmed in flight.** DDS will be intricately integrated with Law Enforcement entities. and Military/National Guard.” EX1006, page 23.

“**Drone Defense Systems improves on any system by defending against Rogue Drones, by implement an ability to ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses and according to the rules of engagement (these rules can be customized for any protected area) it creates a countermeasure that will disarm, intercept, Return to Sender, or force land a rogue drone.**” EX1006, page 23.

APPENDIX B

Falk (EX1011), Claim 1	U.S. Provisional Application No. 62/301,858 filed March 1, 2016 (EX1012) (the “’858 Provisional”)
[1a] A beacon attached to an unmanned aerial vehicle, the unmanned aerial vehicle including a control system, a sensory system, and a communications system, the beacon comprising:	The ’858 Provisional supports element [1a] verbatim. “A beacon attached to an unmanned aerial vehicle, the unmanned aerial vehicle including a control system, a sensory system, and a communications system, the beacon comprising:” EX1012, page 23 (Claim 5).
[1b] an attachment mechanism configured to securely and removably attach the apparatus to the unmanned aerial vehicle;	The ’858 Provisional supports element [1b] verbatim. “an attachment mechanism configured to securely and removably attach the apparatus to the unmanned aerial vehicle;” EX1012, page 23 (Claim 5).
[1c] an unmanned aerial vehicle communications module configured to provide commands and transmit and receive information to and from the unmanned aerial vehicle through the unmanned aerial vehicle communications system;	The ’858 Provisional supports element [1c] verbatim. “an unmanned aerial vehicle communications module configured to provide commands and transmit and receive information to and from the unmanned aerial vehicle through the unmanned aerial vehicle communications system;” EX1012, page 23 (Claim 5).

[1d] a remote communications module configured to participate on at least one wireless communications system, the remote communications module being configured to transmit and receive information across the at least one wireless communications system to and from a remote operator;	The '858 Provisional supports element [1d] verbatim. “a remote communications module configured to participate on at least one wireless communications system, the remote communications module being configured to transmit and receive information across the at least one wireless communications system to and from a remote operator;” EX1012, page 24 (Claim 5).
[1e] a beacon control system configured to receive information and commands from the remote communications module and to transform the information and commands for compatibility with the unmanned aerial vehicle, the beacon control system further being configured to transmit the transformed information and commands to the unmanned aerial vehicle through the unmanned aerial vehicle communications module;	The '858 Provisional supports element [1e] verbatim. “a beacon control system configured to receive information and commands from the remote communications module and to transform the information and commands for compatibility with the unmanned aerial vehicle, the beacon control system further being configured to transmit the transformed information and commands to the unmanned aerial vehicle through the unmanned aerial vehicle communications module;” EX1012, page 24 (Claim 5).

[1f] wherein the beacon control system is further configured to receive information from the unmanned aerial vehicle through the unmanned aerial vehicle communications module and to transform the information for transmission over the at least one wireless communications system; and	The '858 Provisional supports element [1f] verbatim. “wherein the beacon control system is further configured to receive information from the unmanned aerial vehicle through the unmanned aerial vehicle communications module and to transform the information for transmission over the at least one wireless communications system; and.” EX1012, page 24 (Claim 5).
[1g] wherein the remote communications module transmits the transformed information to the remote operator.	The '858 Provisional supports element [1g] verbatim. “wherein the remote communications module transmits the transformed information to the remote operator.” EX1012, page 24 (Claim 5).

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 1st day of September, 2026, **PETITIONERS' SUBMISSION REGARDING THE AUGUST 27, 2026 ORDER (PAPER 42)** was served by email on the following counsel for Patent Owner:

swadekar@princelobel.com

alesperance@princelobel.com

mvella@princelobel.com

jhall@princelobel.com

msaunders@princelobel.com

airspacedrone@princelobel.com

Respectfully submitted,

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Counsel for Petitioners

Date: September 1, 2026

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com