

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. IPR2025-00525

Patent 10,713,959

**PETITIONERS' OPPOSITION TO PATENT OWNER'S NON-
CONTINGENT REVISED MOTION TO AMEND**

TABLE OF CONTENTS

I.	THE SC LACKS WRITTEN DESCRIPTION SUPPORT.....	1
A.	Elements [22.e] and [22.f].....	1
II.	THE SC IS INDEFINITE	5
A.	The term “low altitude aircraft” is indefinite	5
B.	The term “the received information” is indefinite	6
III.	THE AMENDMENT IMPERMISSIBLY BROADENS THE SC.....	7
IV.	SC 22 IS OBVIOUS.....	7
1.	Ground 5B: Beard, Viggiano, and Hayes.....	9
2.	Grounds 6B and 7B	17
3.	Ground 8B: Gong, Wang-II, Viggiano, and Hayes.....	21
4.	Ground 9B	24
5.	Grounds 10B, 11B, and 12B	25

LIST OF EXHIBITS

Ex. No.¹	Description
1001	U.S. Patent No. 10,713,959 to Foina <i>et al.</i> , “Low Altitude Aircraft Identification System” (the “’959 Patent”)
1002	File History for U.S. Patent No. 10,713,959
1003	Declaration of Dr. Girish Chowdhary
1004	Complaint for Patent Infringement, <i>Airspace Systems, Inc. v. Dedrone Holdings, Inc.</i> , Case No. 1-24-cv-01625 (E.D. VA), September 16, 2024
1005	U.S. Patent No. 10,192,451 to Foina <i>et al.</i> , “Low Altitude Aircraft Identification System,” (the “’451 Patent”) filed December 12, 2017
1006	International Publication No. WO2016/201359 A1 filed on June 10, 2016 as International Application No. PCT/US2016/037071 (the “’071 Application”)
1007	U.S. Provisional Application No. 62/175,153 to Foina <i>et al.</i> , “A low altitude aircraft identification system” (the “’153 Provisional”), filed June 12, 2015
1008	U.S. Patent No. 10,733,894 to Beard <i>et al.</i> , “Direct-Broadcast Remote Identification (RID) Device for Unmanned Aircraft Systems (UAS),” (“ <i>Beard</i> ”) filed February 26, 2018 and issued August 4, 2020
1009	U.S. Provisional Application No. 62/480,031 to Beard, “Remote Identification” (“ <i>Beard Provisional</i> ”), filed March 31, 2017
1010	U.S. Patent Application Publication No. 2016/0253907 to Taveira, “Systems and Method for Restricting Drone Airspace Access,” (“ <i>Taveira</i> ”) filed January 29, 2015 and published September 1, 2016
1011	International Publication No. WO2016/078093 A1 to Wang <i>et al.</i> , “System and Methods for Managing Unmanned Aerial Vehicles,” (“ <i>Wang</i> ”) filed November 21, 2014 and published May 26, 2016

¹ Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to Exhibits 1002, 1007, 1016, and 1028 are made with reference to the Bates-stamped pagination; citations to other exhibits are made to the page number of the document itself.

1012	International Publication No. WO2016/154949 A1 to <i>Gong et al.</i> , “Authentication Systems and Methods for Generating Flight Regulations,” (“ <i>Gong</i> ”) filed March 31, 2015 and published October 6, 2016
1013	U.S. Patent Application Publication No. 2016/0127890 to <i>Qi et al.</i> , “Apparatus, System and Method of Protecting a Service Identifier,” (“ <i>Qi</i> ”) filed December 24, 2014 and published May 5, 2016
1014	International Publication No. WO2015/043123 A1 to <i>Wang et al.</i> , “Data Communication Systems and Methods,” (“ <i>Wang-II</i> ”) filed January 14, 2014 and published April 2, 2015
1015	Claim Listing of Challenged Claim
1016	File History for U.S. Patent No. 10,192,451
1017	First Amended Complaint for Patent Infringement, <i>Airspace Systems, Inc. v. Dedrone Holdings, Inc.</i> , Case No. 1-24-cv-01625 (E.D. VA), October 30, 2024
1018	Airspace Systems, Inc.’s Opposition to Defendants’ Rule 12(b)(6) Motion to Dismiss, <i>Airspace Systems, Inc. v. Dedrone Holdings, Inc.</i> , Case No. 1-24-cv-01625 (E.D. VA), January 13, 2025
1019	U.S. Patent Application Publication No. 2014/0337633 <i>et al.</i> , “System and Method for Indicating a Service Set Identifier,” filed May 7, 2014 and published November 13, 2014
1020	U.S. Patent Application Publication No. 2006/0236376 to <i>Liu et al.</i> , “Wireless Security Using Media Access Control Address Filtering with User Interface,” filed April 1, 2005 and published October 19, 2006
1021	Kayton, Myron and Fried, Walter, <i>Avionics Navigation Systems</i> , John Wiley and Sons, 1997.
1022	Stipulation email on May 29, 2025
1023	Second Declaration of Dr. Girish Chowdhary
1024	U.S. Patent Application Publication 2007/0239986 to <i>Viggiano et al.</i> , “Secure ADS-B Authentication System and Method,” (“ <i>Viggiano</i> ”) filed April 7, 2006 and published October 11, 2007
1025	U.S. Patent No. 9,875,660 to <i>Byers et al.</i> , “Multi-Modal UAV Certification,” (“ <i>Byers</i> ”) filed March 28, 2016 and issued January 23, 2018
1026	Transcript of Deposition of Dr. Nikolaos Papanikolopoulos
1027	Third Declaration of Dr. Girish Chowdhary

U.S. Patent No. 10,713,959

1028	<i>Who goes there: Friend or Foe?</i> , Office of Technology Assessment, Congress of the United States, Washington, DC, U.S. Government Printing Office, June 1993 (“FF”)
1029	Declaration of Dr. Sylvia Hall-Ellis
1030	U.S. Patent No. 10,380,775 to Hayes, “Map Declutter,” (“Hayes”), filed August 6, 2014, issued August 13, 2019

I. THE SC LACKS WRITTEN DESCRIPTION SUPPORT

A. Elements [22.e] and [22.f]

In a 180-degree reversal from its prior MTA, PO says the *secure identifier* is (1) sent from a *remote portable detection system* **up** to the *aircraft* and (2) comprises a *specified excitation enabling disambiguation of the first low-altitude aircraft*. RMTA (Paper 26), 5-7, 11-12; MTA (Paper 16), 8-9. PO cannot show sufficient support for these limitations because they (1) seek to reverse the only described directional flow of the *secure identifier*; (2) rely upon **light array** embodiments that do not support the claimed requirement that the *secure identifier* be received by *the radio communication module*; and (3) conflate the *secure identifier* with generic light beam disclosures. EX1027, ¶30.

First, the specification lacks any description of a *secure identifier* being received by an aircraft on the uplink—i.e., from a ground station (*remote portable detection system*). The term *secure identifier* does not even appear in the specification. EX1001. The only contextual clue provided by the intrinsic record is found in the patent’s dependent claim 3, which states that the *secure identifier* comprises a *rotating SSID*. *Id.*, Claim 3. When the specification describes this SSID, it describes it exclusively as transmitted from the aircraft **down** to the ground station. EX1001, 1:28-31, 1:45-2:3, 11:66-12:62, Figs. 9-13. Nowhere does the patent describe the SSID—or any other *secure identifier*—as transmitted from a *remote*

portable detection system up to the aircraft, as PO now tries to claim. RMTA, 5-7. PO thus cannot show possession of a secure identifier comprising a specified excitation that is received by the radio communication module [of the low-altitude aircraft] . . . from a remote portable detection system. Id.; EX1027, ¶30.

Second, PO improperly relies on **optical embodiments** to satisfy limitations tied to a **radio receiver**. Element [22.f] requires the *radio communication module* to receive the *specified excitation*. RMTA, 5-7. Yet, every disclosure PO cites in its RMTA to support this element relates to receiving a physical beam via a **photo sensor or light array**. RMTA, 5 (citing EX2015 at 3:22-26 (“The identification box has a *photo sensor* configured to receive **external signals**. In case *the photo sensor* is **excited with a high luminous beam** . . . such as a *laser beam*, the identification box may change its behavior...”), 3:31-4:4 (“it is just a matter of directing a **specific wavelength and modulated light beam emitter** to one of the aircrafts . . . and receive directional data *through the light sensor*”), 9:6-12 (“In order to activate (e.g., **excite**) the *identification box light sensor 19* . . . This *beam*, when captured by *the light sensor 19* . . .”), 9:15-21 (“The **identification box light emitters 3 and light sensor 4** of the identification box . . .”) (emphases added in bold italics, non-italic bold in original). All of those excerpts describe receiving *excitation* through a **photo or light sensor**, not a *radio communication module* as claimed. And the cited reference at 9:15-21 to generate “exchange [of] information” through RF via a

“duplex communication” does not provide written description support of receiving the claimed *specified excitation enabling disambiguation . . . wherein the specified excitation causes the first low-altitude aircraft to change a behavior thereof*. This general reference to exchanging general information over RF does not disclose receiving the specifically-claimed *secure identifier comprising a specified excitation*.... EX1027, ¶¶31-33.

Third, PO further incorrectly conflates two completely distinct concepts: the claimed *secure identifier* and disclosures about a generic light beam. The amendment requires a *secure identifier* that comprises a *specified excitation* and that *causes the first low-altitude aircraft to change a behavior thereof*. RMTA, 5-7. PO points solely to descriptions of **a light beam**—disconnected from any discussion of a *secure identifier*—as providing support. *Id.* But this new combination of concepts appears nowhere in the specification, and PO’s attempt to stitch it together fails. The patent never describes a *secure identifier* as comprising *an excitation enabling disambiguation* of the aircraft and that *causes the first low-altitude aircraft to change a behavior thereof*. The Board’s Institution Decision (“ID,” Paper 13) preliminarily construed *secure identifier* as a “credential that can be used to securely verify the identity of a device.” ID, 6-10. Nothing in the patent connects the *secure identifier* or that term as construed to such an excitation and change in aircraft behavior. EX1027, ¶¶34-35. Moreover, PO’s citations to generic light beams do not support

the *secure identifier*. Patent Owner relies solely on passages describing how a “photo sensor is excited with a high luminous beam” to trigger a behavior change. RMTA, 5 (citing EX2015 at 3:22-26 (describing that the sensor is excited with a “**high luminous beam**” without any connection to a *secure identifier*), 3:31-4:4 (same), 9:6-12 (same), 9:15-21 (providing a general description of two-way communication) (emphasis added). But an aircraft receiving a laser beam or light beam to provoke a physical reaction does not support the reception, by the claimed *radio communication module*, of a *secure identifier* or, as construed, a “credential that can be used to securely verify the identity of a device.” *Id.*; EX1027, ¶36. By stitching the *secure identifier* limitation together with the *specified excitation enabling disambiguation* and that *causes the first low-altitude aircraft to change a behavior thereof*, PO introduces new matter lacking support. EX1027, ¶36.

Petitioners further note that, for the same reasons discussed in the Petition, element [22.e] is not adequately supported by the ’153 Prov. (EX2016), and the SC is not entitled to claim priority to PCT/US2016/037071 (“the ’071 Application”). Petition (Paper 1, “Pet.”), 7-16. The Board recognized this in the ID, stating that “the ’153 Provisional and ’071 Application lack adequate written description support for the ‘secure identifier’ limitation of claim 21,” which is also recited in the SC. ID, 11-14. The RMTA does not properly address the Board’s analysis of the ID or the priority issues raised by the Petition. Instead, the RMTA generically states that the

“secure identifier” recited by the SC “is fully supported by both the ’406 App. and the ’153 provisional” and refers to Section IV of the RMTA. RMTA, 11. But PO’s conclusory statement does not change the Board’s correct determination in the ID. ID, 11-14. The SC recites the same “secure identifier” as original claim 21 and elements [22.e] and [22.f] describe what the secure identifier also “comprises” and how it is “utilized”—not what the term itself means (as construed in the ID). RMTA, 5-7. Thus, the SC still suffers from the same written description issues recognized by the Board regarding original claim 21. And PO’s reference to RMTA Section IV is without merit because, as discussed above, the RMTA’s cited portions for [22.e] and [22.f] (contained in Section IV) do not provide support. PO failed to demonstrate [22.e] and [22.f] have sufficient written description support. EX1027, ¶37.

II. THE SC IS INDEFINITE

A. The term “*low altitude aircraft*” is indefinite

The SC recites a *low-altitude aircraft*. RMTA, 3-10. “[L]ow-altitude” is a term of degree, and the specification provides no objective standard for determining what constitutes *low altitude*, rendering the SC indefinite. EX1027, ¶¶38-39. “Although ‘terms of degree are [not] inherently indefinite,’ the patent must provide ‘some standard for measuring that degree.’” *GE Lighting Sols., LLC v. Lights of Am., Inc.*, 663 F. App’x 938, 940 (Fed. Cir. 2016). “[T]he patent must provide that additional information in the form of ‘objective boundaries.’” *Id.* Relative modifiers

like “high” are terms of degree that have been held indefinite when the intrinsic record lacks objective guidance. *J.R. Simplot Co. v. McCain Foods USA, Inc.*, 713 F. Supp. 3d 904, 942 (D. Idaho 2024) (“high electric field” an indefinite term of degree.); *Bayer Intell. Prop. GmbH v. Warner Chilcott Co., LLC*, No. 12-1032-GMS, 2015 WL 1849015, at *1 (D. Del. Apr. 21, 2015); *Jaguar Land Rover Ltd. v. Bentley Motors Ltd.*, No. 2:18-cv-320, 2020 WL 7010227, at *6 (E.D. Va. Nov. 25, 2020). “**Low altitude**” aircraft is a classic term of degree; whether an altitude is *low* or not is a matter of degree. The problem, however, is the specification does not provide any objective boundaries for determining when an altitude is “*low*” or not in the context of aircraft. EX1027, ¶39. The patent recites “airborne objects at a low altitude,” but does not describe any objective boundary for a “low” altitude. EX1001, 1:29-31, 4:37-40. No objective standard exists; the term is indefinite. EX1027, ¶39.

B. The term “the received information” is indefinite

Element [22.c] recites *wherein the radio communication module is configured to receive a radio signal and store the received information in a storage*. RMTA, 4 (emphasis added). [T]he received information lacks antecedent basis. There is no prior recitation of any *information* that is *received*. Use of *the received information* causes confusion as the SC previously recites *identification information*; it is unclear whether these pieces of *information* are the same or different. *Id.*; RMTA, 3-4. If the *radio signal* that is *receive[d]* is considered the *received information*, this is wrong.

EX1027, ¶40. A POSITA would not have considered these the same because they are different terms, connoting different meanings. *Id.*

III. THE AMENDMENT IMPERMISSIBLY BROADENS THE SC

Original claim 22 recited a *device* comprising a *radio communication module* configured to *receive a **received** radio signal*. EX1001, Claim 22 (emphasis added). The SC removes the term “received.” RMTA, 4. This changes meaning and impermissibly broadens. “[R]eceived” limited the *radio communication module* to receive only radio signals the claimed *device* had actually received—e.g., signals of a compatible “type” and “range” receivable by the *device*. *Id.* The patent explains the device can receive “wireless signals of various types and range.” EX1001, 13:23–29. By deleting *received*, the amendment removes that limitation. EX1027, ¶29. The SC now covers the *radio communication module* receiving *any* radio signal, including signals of a type the *device* could not have received in the original claim because they were incompatible. *Id.*; RMTA, 4. This broadening is improper. *Sisvel Int’l S.A. v. Sierra Wireless, Inc.*, 81 F.4th 1231, 1240–41 (Fed. Cir. 2023). Nothing supports that this is “a typographical correction.” RMTA, 2; EX1027, ¶29.

IV. SC 22 IS OBVIOUS

SC limitations added via RMTA and relevant original claim limitations are addressed; unaddressed original limitations are addressed in the Petition. Elements that are indefinite and/or lack written description support are addressed based on

Petitioners' understanding of PO's position and as best understood by a POSITA.

Ground	SC	35 U.S.C. §	Prior Art
5B	22	103	Beard, Viggiano, and Hayes
6B	22	103	Taveira, Wang, Gong, Viggiano, and Hayes
7B	22	103	Taveira, Qi, Gong, Viggiano, and Hayes
8B	22	103	Gong, Wang-II, Viggiano, and Hayes
9B	22	103	Beard, Viggiano, Hayes, and FF
10B	22	103	Taveira, Wang, Gong, Viggiano, Hayes, and FF
11B	22	103	Taveira, Qi, Gong, Viggiano, Hayes, and FF
12B	22	103	Gong, Wang-II, Viggiano, Hayes, and FF

Grounds 5B-8B rely on the Petition's original grounds and add Viggiano and Hayes, and grounds 9-12 rely on the Petition's original grounds and add Viggiano, Hayes, and FF. PO asserts a priority date of June 12, 2015. RMTA, 2-11. Petitioners disagree. Section I.A; Pet., 7-16. At best, the '959 Patent's priority date is October 1, 2017, the filing date of U.S. Provisional Application No. 62/566,450 (which Petitioner assumes but does not concede). *Id.* FF (publicly available by at least December 13, 1993) is prior art under 35 U.S.C. §102(a)(1), Viggiano (published October 11, 2007; filed April 7, 2006) is prior art under 35 U.S.C. §102(a)(1) and (a)(2), and Hayes (filed August 6, 2014) is prior art under 35 U.S.C. §102 (a)(2). EX1024, Cover; EX1028, 1; EX1029; EX1030, Cover. As FF, Viggiano, and Hayes

address aircraft identification techniques, they are highly relevant to the '959 Patent. EX1027, ¶¶43-49; EX1001, 1:28-31, 2:27-29; EX1024, Abstract, ¶¶0002, 0012-0018, 0024-0027, Figs. 1, 3; EX1028, 49, 62-66; EX1030, 5:38-67, Fig. 6.

1. Ground 5B: Beard, Viggiano, and Hayes

Motivation to Combine: A POSITA would have been motivated to combine Beard, Viggiano, and Hayes with a reasonable expectation of success. EX1027, ¶50. Viggiano describes authenticating aircraft identity by transmitting a challenge 12 from authenticator 10 to the aircraft to provoke an authentication response. EX1024, ¶¶0012-0015, Fig. 1. Challenge 12 is formed from a “unique identifier” that can be “random values.” *Id.*, ¶¶0012-0013, Fig. 1. Upon receiving challenge 12, the aircraft forms an “authentication challenge response 18” including a message authentication code (MAC) 38, which the aircraft’s ADS-B transmitter transmits to authenticator 10. *Id.*, ¶¶0013-0014. Authenticator 10 receives response 18 and its MAC 38, and forms its own MAC 58 using, among other information, the locally generated unique identifier. *Id.*, ¶¶0013-0015. Authenticator 10 then uses comparator 60 to compare MACs 38 and 58 to determine whether the “identity of the ADS-B transmitter” (and thus, the transmitting UAV’s identity) is authenticated, where matching MACs indicates an authenticated identity. *Id.* If two or more consecutive comparisons fail, then authenticator 10 “notifies a responsible higher command authority of the authentication failures” so the authority can “respond appropriately.” *Id.*

Authenticator 10 can also issue an “alert” that is displayed on other “aircraft, vehicles, vessels or stations.” *Id.* Hayes teaches that a UAV associated with an “alert” is caused to be more clearly displayed on a user interface—by removing other detected and displayed UAVs from the interface so that the UAV associated with the alert is more visible. EX1030, 5:38-67, Fig. 6. Thus, as combined, the Beard-Viggiano-Hayes system would have provided the predictable result in which Beard’s first unmanned aerial system (UAS) RF transceiver (1) receives from Beard’s receiver a challenge 12, (2) determines to transmit a challenge response, and (3) transmits the challenge response to Beard’s receiver, and the receiver—based on the response and a subsequent consecutive authentication failure alert—modifies its displayed user interface, causing other detected and displayed UASs to be removed from the interface so that the first UAS is more clearly displayed. EX1024, ¶¶0002, 0011-0015, Figs. 1-3, Claims 1, 5, 8, 21, 39; EX1030, 5:38-67, Fig. 6; Pet., 29-39; EX1008, Abstract, 3:9-19, 3:30-36, 5:9-10, 5:33-51, 5:41-57, 6:23-25, 6:56-60, 7:11-17, 7:34-51, 8:28-32, 8:39-42, 9:8-12, 9:67-10:12, 10:12-20, Fig. 4B; EX1009, 2-9, 11, 14, 15, Fig. 2; EX1027, ¶¶51-52. A POSITA would have been motivated to combine in this manner because the use of false or fraudulent identity information by aircrafts was a known problem. EX1024, ¶¶0003-0007; EX1027, ¶53. Viggiano addresses this problem and furthers Beard’s own verification teachings, providing a specific technique for aircraft identity verification that prevents “unauthorized third

parties” from “enter[ing] a given air traffic control region by broadcasting false identification data.” EX1024, ¶0004; EX1027, ¶53. Viggiano and Hayes provide implementation details for performing Beard’s verification, using a challenge-response technique, and displaying subsequent results, which would have been straightforward and routine to implement. EX1008, 3:30-36, 5:41-57, 8:39-42, 9:8-12, 10:12-20; EX1009, 5-8, 11; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; EX1030, 5:38-67, Fig. 6; EX1027, ¶53. These teachings provide an additional layer of security, benefiting the combination. *Id.* Moreover, Beard and Viggiano determine accurate aircraft identity and utilize ADS-B for aircraft data transmissions, further demonstrating their compatibility and complementary nature. EX1008, 2:22-49, 2:66-3:36, 4:61-5:7, 6:20-29, 7:11-26; EX1009, 2-5, 7-11, 12-14; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; EX1027, ¶54. Viggiano also explains that consecutively failed authentications causes issuance of an “alert that is displayed” by a station. EX1024, ¶¶0014-0015. Hayes teaches that a UAV associated with an “alert” is caused to be more clearly displayed on an interface—by removing other detected and displayed UAVs from the interface so that the UAV associated with the alert is more visible. EX1030, 5:38-67, Fig. 6. As such, Viggiano and Hayes teach that Beard’s receiver, which detects multiple UASs and displays their identification and position data on a user interface (Pet., 35-39), would have had a modifiable user interface that more clearly displays a UAV

associated with a failed authentication alert by removing other detected and displayed UAVs from the interface. *Id.*; EX1030, 5:38-67; EX1024, ¶¶0014-0015; EX1027, ¶54. Due to the compatibility of these teachings, the straightforward nature of the combination, and the routine modifications that would have been necessary (e.g., providing the known challenge-response protocol as taught by Viggiano, and the modification of user interface as taught by Hayes), there would have been a reasonable expectation of success. *Id.* [22.pre], [22.b], [22.d], [22.h]: Beard describes multiple UAS 102 (102a, 102b, 102c, etc) are present in an airspace and are detected by Beard’s receiver, and a first of these UAS forms a *first low-altitude aircraft* as claimed. EX1008, 2:22-23, 7:52-8:51, 8:51-61, 9:3-58, Fig. 4B; EX1009, 1, 2, 4-7, 14-15, Fig. 2; EX1027, ¶55; Pet. 24-28, 29-31, 34, 37-39. The remaining aspects of elements [22.pre], [22.b], [22.d], [22.h] are taught as in the Pet. and in the sections of this ground below. *Id.*; Section IV.1, *infra.* [22.c]: Beard’s remote identification (RID) device attached to an unmanned aircraft system (UAS) includes an RF transceiver (*radio communication module*). Pet., 29-31. Beard’s RF transceiver (*radio communication module*) can “‘listen’ for other proximate UAS within range, receiving identifier signals transmitted by another RID device (100a) aboard the proximate UAS and relaying the received signals throughout the RID coverage area of the RID device 100.” EX1008, 7:34-42; EX1009, 14; Pet., 31-34. The RID devices can communicate on different radio frequencies. Pet., 28-31.

Accordingly, Beard teaches “*wherein the radio communication module is configured to receive a radio signal.*” EX1027, ¶56. Beard discloses to “*store the received information in a storage.*” *Id.*; Pet., 31-34. If “*the received information*” is interpreted to refer to the “*identification information associated with the first low-altitude aircraft*” recited in [22.b], Beard discloses that the RID device can “store[] to memory” the “current position of the UAS 102 and identification data” of the UAS associated with the RID device. *Id.*; EX1008, 5:44-46, 7:45-47; EX1009, 11, 15; EX1003, ¶125; Pet., 31-34; EX1027, ¶57. If “*the received information*” is interpreted to refer to information associated with the “*radio signal*” recited in [22.c], Beard discloses that “memory 106 of the RID device 100 may serve as an ad hoc black box data recorder, storing data regarding the UAS 102 ***as well as other nearby UAS, based on received identifier signals.***” *Id.*; EX1008, 7:45-48 (emphasis added), 7:48-51; EX1009, 15; EX1003, ¶126; Pet., 31-34; Section IV.1 ([22.c]).

[22.e]: Beard’s RF transceiver forms the “*radio communication module.*” Pet., 29-31. The Beard-Viggiano-Hayes combination teaches that Beard’s RF transceiver (*the radio communication module*) of the first UAS receives from Beard’s receiver (“*remote portable detection system*”) an “authentication challenge 12” comprising a “unique identifier” having “random values” generated by a random number generator, where the “unique” aspect of the unique identifier and random values provide security such that “an attacker cannot ‘learn’ a valid response by observing

the challenges 12,” and the RF transceiver further uses challenge 12 (and its unique identifier) to prepare an authentication challenge response (*the radio communication module is configured to utilize a secure identifier*). *Id.*; Section IV.1 (MTC); EX1024, ¶¶0012-0013; Pet., 35-39; EX1027, ¶58. Indeed, by using a unique identifier (e.g., a random number) for each challenge, each challenge 12 is continually different and an attacker cannot learn it, which provides that the challenge 12 is *secure*. EX1024, ¶¶0012-0013; EX1027, ¶58. The challenge 12 (*secure identifier*) is or includes an excitation because it causes Beard’s RF transceiver to prepare and transmit the challenge response (*secure identifier comprising a specified excitation*). EX1024, ¶¶0012-0013; Section IV.1 (MTC); Pet., 29-31; EX1027, ¶58. This is because the challenge is part of Viggiano’s taught “challenge-response methodology” that is used to authenticate aircraft identity. EX1024, ¶¶0012-0013; EX1027, ¶¶58-59. Moreover, the challenge response that is transmitted by Beard’s RF transceiver allows for the first UAS to be distinguished from among multiple detected UAVs and highlighted for display (*enabling disambiguation of the first low-altitude aircraft from other detected low-altitude aircraft*), as taught by Hayes. *Id.*; Pet., 29-31; EX1030, 5:38-67, Fig. 6; Section IV.1 (MTC). Specifically, the combination teaches that the challenge response is transmitted by Beard’s RF transceiver to Beard’s receiver, and the receiver attempts authentication of the first UAS’s identity based on the response. EX1024, ¶¶0012-

0015; Pet., 29-31, 35-39; Section IV.1 (MTC); EX1027, ¶59. Consecutive failures of the authentication causes issuance of “an alert” that triggers a modification of the displayed user interface of Beard’s receiver, causing other detected and displayed UASs to be removed from the interface and the first UAS to thus be more clearly displayed. *Id.*; EX1030, 5:38-67, Fig. 6. Beard’s receiver detects multiple UASs and displays their identification and position data. Pet., 35-39. Because the challenge 12 (*secure identifier*) includes the “unique identifier” having “random values” generated by a random number generator, where the “unique” aspect of the unique identifier provides that “an attacker cannot ‘learn’ a valid response by observing the challenges 12, and challenge 12 is used to verify the identity of the first UAS, it satisfies the Board’s *secure identifier* construction of “a credential that can be used to securely verify the identity of a device, such as an airborne object or ground-based transmitter.” EX1024, ¶¶0012-0015; Paper 13 at 10; Pet., 29-31, 35-39; Section IV.1 (MTC); EX1027, ¶60. **[22.f]:** Beard’s receiver forms a “*remote portable detection system*.” Pet., 35-39. The Beard-Viggiano-Hayes combination teaches *utilizing the secure identifier* comprises Beard’s RF transceiver receiving challenge 12 that includes the excitation (*comprises receiving by the radio communication module the specified excitation*) from Beard’s receiver (*from the remote portable detection system*). Section IV.1 ([22.e]); EX1027, ¶61. This excitation (*the specified excitation*) causes the first UAS to change a behavior in that the first UAS is

triggered to prepare and transmit a challenge response (*wherein the specified excitation causes the first low-altitude aircraft to change a behavior thereof*). Section IV.1 ([22.e]); EX1027, ¶61. **[22.g]:** Beard's receiver forms "*the remote portable detection system*," and the remaining aspects of [22.g] are addressed in the Petition. Pet., 35-39; EX1027, ¶62. **[22.i]:** Multiple UAS 102 are present in an airspace and detected by Beard's receiver (forming *the plurality of different low-altitude aircrafts*), and one of these UAS forms the *first low-altitude aircraft*, teaching that *the plurality [is] comprising the first low-altitude aircraft*. Section IV.1 ([22.pre] et al.); Petition, 37-39; EX1027, ¶63. Upon consecutive authentication failures for the first UAS, Beard's receiver (*the remote portable detection system*) modifies its user interface display such that other detected and displayed UAS are removed from the interface and the first UAS is thus more clearly displayed (*is configured to disambiguate the first low-altitude aircraft from the other detected low-altitude aircraft of the plurality*). Pet., 35-39; Sections IV.1 ([22.e], [22.f], [22.g], MTC); EX1027, ¶63. Moreover, this changing the form of display such that first UAS is more clearly displayed relative to the other detected UASs (*disambiguate the first low-altitude aircraft from the other detected low-altitude aircraft of the plurality*) is based on the first UAS's triggered authentication response (*based on the changed behavior of the first low-altitude aircraft*) to the authentication challenge that causes the first UAS to have failed consecutive

authentications. Section IV.1 ([22.e], [22.f], MTC); EX1027, ¶63. The remaining aspects of [22.i] are addressed in the Petition. Pet., 37-39; EX1027, ¶63.

2. Grounds 6B and 7B

Motivation to Combine (MTC): A POSITA would have been motivated to combine Taveira, Wang, and Gong/Taveira, Qi, and Gong, and further motivated to combine each combination with Viggiano and Hayes for the same reasons discussed for Viggiano and Hayes in Section IV.1 (MTC). Pet. at 40-45, 60-62; EX1027, ¶64. The combinations would have provided the same predictable result as discussed in Section IV.1 (MTC), except Taveira's first drone 100 having radio module 130 is what receives a challenge 12 from wireless communication device 170 and determines to transmit and transmits a response, and wireless communication device 170 is what receives the response and modifies its displayed user interface based on the response and subsequent alert. Section IV.1 (MTC); EX1024, ¶¶0002, 0011-0015, Figs. 1-3, Claims 1, 5, 8, 21, 39; EX1030, 5:38-67, Fig. 6; Pet. at 40-45, 49-60, 60-64; EX1003, ¶¶138-146, 172-176; EX1027, ¶64. **[22.pre], [22.b], [22.d], [22.h]:** Taveira and Gong teaches multiple drones 100 that are detected and displayed by Taveira's wireless communication device 170, and a first of these drones 100 forms a *first low-altitude aircraft* as claimed. Pet. 45-50, 53, 55-60, 62; EX1027, ¶65. The remaining aspects of elements [22.pre], [22.b], [22.d], [22.h] are taught as in the Pet. and in the sections of this ground below. *Id.*; Section IV.2, *infra*.

[22.c]: Taveira’s radio module 130 forms a *radio communication module*. Pet. at 49-50, 62. Radio module 130 receives RF signals from other devices (*wherein the radio communication module is configured to receive a radio signal*). Pet., 50-53, 62; EX1027, ¶66. The combinations each teach to “*store the received information in a storage.*” *Id.* If “*the received information*” refers to the “*identification information associated with the low-altitude aircraft*” of [22.b], the combinations disclose storing identification data associated with the drone. *Id.*; Pet., 50-53, 62. If “*the received information*” refers to information associated with the “*radio signal*” of [22.c], the combinations disclose such information is stored in memory unit 121 of drone 100. *Id.* **[22.e]:** The combinations teach that radio module 130 (*the radio communication module*) of the first drone 100 receives from wireless communication device 170 (“*remote portable detection system*”) an “authentication challenge 12” comprising a “unique identifier” having “random values” generated by a random number generator, where the “unique” aspect of the unique identifier provides that “an attacker cannot ‘learn’ a valid response by observing the challenges 12, and the radio module 130 further uses challenge 12 (and its unique identifier) to prepare an authentication challenge response (*the radio communication module is configured to utilize a secure identifier*). Pet., 40-45, 49-60, 60-64; Sections IV.2 (MTC), ([22.c]); EX1024, ¶¶0012-0013; EX1027, ¶67. The challenge 12 (*secure identifier*) includes an excitation that causes radio module 130 to prepare and

transmit the challenge response (*secure identifier comprising a specified excitation*). EX1024, ¶¶0012-0013; Section IV.2 (MTC); Pet. at 40-45, 49-60, 60-64; EX1027, ¶68; Section IV.1 ([22.e]). Moreover, the challenge response that is transmitted by radio module 130 allows for the first drone 100 to be distinguished from among multiple detected drones 100 and highlighted for display (*enabling disambiguation of the first low-altitude aircraft from other detected low-altitude aircraft*), as taught by Hayes. *Id.*; Pet. at 40-45, 49-60, 60-64; EX1030, 5:38-67, Fig. 6; Section IV.2 (MTC). Specifically, the combination teaches that the challenge response is transmitted by radio module 130 to wireless communication device 170, and the wireless communication device 170 attempts authentication of the first drone 100's identity based on the response. EX1024, ¶¶0012-0015; Pet. at 40-45, 49-60, 60-64; Section IV.2 (MTC); EX1027, ¶69. Consecutive failures of the authentication cause "an alert" to issue that triggers a modification of the displayed user interface of wireless communication device 170, causing other detected and displayed drones 100 to be removed from the interface and the first drone 100 to thus be more clearly displayed. *Id.*; EX1030, 5:38-67, Fig. 6. Wireless communication device 170 detects multiple UASs and displays their identification and position data. Pet. at 40-45, 49-60, 60-64. Challenge 12 (*secure identifier*) satisfies the Board's *secure identifier* construction for the same reasons discussed in Section IV.1 ([22.e]). EX1027, ¶70. **[22.f]:** Wireless communication device 170 forms a "*remote portable detection*

system.” Pet., 55-60, 64. The combinations teach *utilizing the secure identifier* comprises radio module 130 (*the radio communication module*) of the first drone 100 receiving challenge 12 including the excitation (*comprises receiving by the radio communication module the specified excitation*) from wireless communication device 170 (*from the remote portable detection system*). Section IV.2 ([22.e]); EX1027, ¶71. This excitation (*the specified excitation*) causes the first drone 100 to change a behavior in that the first drone 100 is triggered to prepare and transmit a challenge response (*wherein the specified excitation causes the first low-altitude aircraft to change a behavior thereof*). Section IV.2 ([22.e]); EX1027, ¶71. **[22.g]:** Wireless communication device 170 forms “*the remote portable detection system.*” Pet., 55-60, 64. The other aspects of [22.g] are also addressed in the Petition. *Id.*; EX1027, ¶72. **[22.i]:** Multiple drones 100 are detected by wireless communication device 170 (*forming the plurality of different low-altitude aircrafts*); one of these drones 100 forms the *first low-altitude aircraft*, teaching *the plurality [is] comprising the first low-altitude aircraft*. Section IV.2 ([22.pre] et al); Petition, 45-50, 53, 55-60, 62; EX1027, ¶73. Upon consecutive authentication failures for the first drone 100, wireless communication device 170 (*the remote portable detection system*) modifies its user interface display so other detected and displayed drones 100 are removed from the interface and the first drone 100 is more clearly displayed (*is configured to disambiguate the first low-altitude aircraft from the other detected*

low-altitude aircraft of the plurality). Pet., 55-60, 64; Sections IV.2 ([22.e], [22.f], [22.g], MTC); EX1027, ¶73. This changing display form so first drone 100 is more clearly displayed relative to the other detected drones (*disambiguate the first low-altitude aircraft from the other detected low-altitude aircraft of the plurality*) is based on the first drone's triggered authentication response (*based on the changed behavior of the first low-altitude aircraft*) to the authentication challenge that causes failed authentications. *Id.* [22.i]'s remaining aspects are addressed in the Pet. at 58-60, 64. EX1027, ¶73.

3. Ground 8B: Gong, Wang-II, Viggiano, and Hayes

Motivation to Combine (MTC): A POSITA would have been motivated to combine Gong and Wang-II, and further motivated to combine with Viggiano and Hayes for the same reasons discussed for Viggiano and Hayes in Section IV.1 (MTC). Pet., 64-66; EX1027, ¶74. The combination would have provided the same predictable result as discussed in Section IV.1 (MTC), except Gong's first UAV communication module/unit is what receives a challenge 12 from Gong's geofencing device and determines to transmit and transmits a response, and the geofencing device is what receives the response and modifies its displayed user interface based on the response and subsequent alert. Section IV.1 (MTC); EX1024, ¶¶0002, 0011-0015, Figs. 1-3, Claims 1, 5, 8, 21, 39; EX1030, 5:38-67, Fig. 6; Pet. at 64-66, 70-78; EX1003, ¶¶188-191; EX1027, ¶74. **[22.pre], [22.b], [22.d], [22.h]:** Multiple

UAVs are detected and displayed by a geofencing device, and a first of these UAVs forms a *first low-altitude aircraft* as claimed. Pet. 64-66, 70-78; EX1027, 75. The remaining aspects of these elements are taught as in the Pet. and in the ground sections below. *Id.*; Section IV.3, *infra.* **[22.e]**: Gong’s communication module/unit (*the radio communication module*) of the first UAV receives from Gong’s geofencing device (“*remote portable detection system*”) an “authentication challenge 12” having the unique identifier as discussed in Section IV.1 ([22.e]), and the communication module/unit further uses challenge 12 (and its unique identifier) to prepare an authentication challenge response (*the radio communication module is configured to utilize a secure identifier*). Pet., 70-78; Sections IV.1 ([22.e]), IV.3 (MTC); EX1028, 63; EX1027, ¶76. The challenge 12 (*secure identifier*) includes an excitation that causes the communication module/unit to prepare and transmit the challenge response (*secure identifier comprising a specified excitation*). EX1024, ¶¶0012-0013; Section IV.3 (MTC); Pet. at 70-78; EX1027, ¶¶76-77. The challenge response received by the geofencing device *enable[es] disambiguation of the first low-altitude aircraft from other detected low-altitude aircraft* for the same reasons discussed in Section IV.1 ([22.e]). *Id.*; Pet. at 70-78; EX1030, 5:38-67, Fig. 6; Sections IV.1[22.e], IV.3 (MTC). The geofencing device attempts authentication of the first UAV’s identity based on the response and consecutive failures of the authentication causes issuance of “an alert” that triggers a modification of the

displayed user interface, in the same way as discussed in Section IV.1 ([22.e]). EX1024, ¶¶0012-0015; Pet. at 70-78; Section IV.3 (MTC); EX1027, ¶77. *Id.*; EX1030, 5:38-67, Fig. 6. The geofencing device detects multiple drones. Pet., 75-78. Challenge 12 satisfies the Board’s *secure identifier* construction for the same reasons discussed in Section IV.1([22.e]). EX1027, ¶78. **[22.f]:** The combination teaches *utilizing the secure identifier* comprises communication module/unit (*the radio communication module*) of the first UAV receiving challenge 12 that includes the excitation (*comprises receiving by the radio communication module the specified excitation*) from geofencing device (*from the remote portable detection system*). Section IV.3 ([22.e]); EX1027, ¶79. This excitation (*the specified excitation*) causes the first UAV to change a behavior in that the first UAS is triggered to prepare and transmit a challenge response (*wherein the specified excitation causes the first low-altitude aircraft to change a behavior thereof*). *Id.* **[22.g]:** The geofencing device forms “*the remote portable detection system*.” Pet., 75-78. The remaining aspects of [22.g] are also addressed in the Petition. *Id.*; EX1027, ¶80. **[22.i]:** Multiple UAVs are detected by Gong’s geofencing device (forming *the plurality of different low-altitude aircrafts*), and one of these UAVs forms the *first low-altitude aircraft*, teaching that *the plurality [is] comprising the first low-altitude aircraft* as claimed. Section IV.3 ([22.pre] et al); Petition, 64-66, 70-78; EX1027, ¶81. Upon consecutive authentication failures for the first UAV, the geofencing device (*the remote portable*

detection system) modifies its user interface display such that other detected and displayed UAV are removed from the interface and the first UAV is thus more clearly displayed (*is configured to disambiguate the first low-altitude aircraft from the other detected low-altitude aircraft of the plurality*). Sections IV.3 ([22.e], [22.f], [22.g], (MTC); Pet., 75-78; EX1027, ¶81. This changing the form of display such that first UAV is more clearly displayed relative to the other detected UAVs (*disambiguate the first low-altitude aircraft from the other detected low-altitude aircraft of the plurality*) is based on the first UAV's triggered authentication response (*based on the changed behavior of the first low-altitude aircraft*) to the authentication challenge that causes failed consecutive authentications. *Id.* The remaining aspects of [22.i] are addressed in the Petition. Pet., 75-78; EX1027, ¶81.

4. Ground 9B

A POSITA would have been motivated to combine Beard, Viggiano, and Hayes (GND 5B) (Section IV.1 (MTC)) and further motivated to combine with FF with a reasonable expectation of success. EX1027, 82. FF discloses “identification friend or foe” authentication techniques used to identify aircraft. EX1028, 31, 49, 62-66. An encrypted “query” (i.e., challenge) is transmitted to an aircraft, asking the aircraft to identify itself, and the aircraft provides a response. *Id.*; EX1027, ¶82. As combined, the Beard-Viggiano-Hayes-FF system would have thus provided the predictable result in which challenge 12 is encrypted, and Beard's first unmanned

aerial system (UAS) RF transceiver receives from Beard's receiver an encrypted challenge 12. Section IV.1 (MTC); EX1028, 49, 63-66; EX1027, ¶¶82-84. This provides an additional security layer to the already secure challenge 12, furthering the combination teachings. *Id.*; EX1024, 0012-0013, Pet., 29-31, 35-39. A POSITA would have had a reasonable expectation of success due to the straightforward nature and use of well-known security techniques (encryption). *Id.* The combination teaches SC 22 for the reasons of Section IV.1, and for elements [22.e] and [22.f], further teaches challenge 12 is encrypted, thus forming a *secure identifier* as claimed and construed by the Board. Sections IV.1 ([22.e], [22.f]); EX1027, ¶¶84-85.

5. Grounds 10B, 11B, and 12B

A POSITA would have been motivated to combine Taveira, Wang, Gong, Viggiano, and Hayes (GND 6B)/Taveira, Qi, Gong, Viggiano, and Hayes (GND 7B)/ Gong, Wang-II, Viggiano, and Hayes (Sections IV.2 and IV.3) and further motivated to combine each combination with FF, for the reasons discussed for FF in Section IV.4. EX1027, ¶¶86-89. The combinations would have provided the predictable result in which challenge 12 is encrypted. *Id.*; Sections IV.2 (MTC), IV.3 (MTC), IV.4 (MTC). The combinations teach SC 22 for the same reasons of Sections IV.2 and IV.3, and for elements [22.e] and [22.f], further teach authentication challenge 12 is encrypted, thus forming a *secure identifier* as claimed and construed. Sections IV.2 ([22.e], [22.f]), IV.3 ([22.e], [22.f]); EX1027, ¶¶86-89.

Respectfully submitted,

BAKER BOTTS L.L.P.

A handwritten signature in black ink, appearing to read "Chad C. Walters". The signature is fluid and cursive, with a long horizontal stroke extending from the end.

Chad C. Walters (Reg. No. 48,022)

Lead Counsel for Petitioners

Date: June 1, 2026

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 1st day of June, 2026,
**Petitioners' Opposition To Patent Owner's Non-Contingent Revised Motion To
Amend and Exhibits 1027-1030** were 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: June 1, 2026

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