

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

TABLE OF CONTENTS

I.	SCS 10-18 LACK WRITTEN DESCRIPTION SUPPORT.....	1
II.	THE SCS ARE UNPATENTABLE	3
A.	SCs 10-18 are Indefinite.....	3
1.	Independent SC 10: [10.d]	3
2.	Independent SC 10: Element [10.g].....	4
B.	SCs 10-18 Are Obvious.....	6
1.	Grounds (GNDs) 7B/7C and 9B/9C: SCs 10-12 and 14-18.....	7
2.	GNDs 8B/8C and 10B/10C.....	19
3.	GNDs 11 and 13.....	19
4.	GNDs 12 and 14.....	25

LIST OF EXHIBITS

Ex. No. ¹	Description
1001	U.S. Patent No. 10,249,199 to Banga, “System and Method for Aerial System Discrimination and Action” (the “199 Patent”)
1002	File History for U.S. Patent No. 10,249,199
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 Application Publication No. 2019/0003807 to Whitmarsh <i>et al.</i> , “UAV Defense System,” (“ <i>Whitmarsh</i> ”) filed December 8, 2016 and published January 3, 2019
1006	U.S. Provisional Application No. 62/267,393 to Whitmarsh <i>et al.</i> , “UAV Defense System,” (“ <i>Whitmarsh Provisional</i> ”), filed December 15, 2015
1007	U.S. Patent Application Publication No. 2007/0239986 to Viggiano <i>et al.</i> , “Secure ADS-B Authentication System and Method,” (“ <i>Viggiano</i> ”) filed April 7, 2006 and published October 11, 2007
1008	U.S. Patent Application Publication No. 2016/0023760 to Goodrich, “Systems and Methods Countering an Unmanned Aerial Vehicle,” (“ <i>Goodrich</i> ”) filed July 16, 2015 and published January 28, 2016
1009	U.S. Patent No. 10,733,894 to Beard <i>et al.</i> , “Direct-broadcast Remote Identification (RID) Device for Unmanned Aircraft Systems (UAS),” filed February 26, 2018 and issued August 4, 2020
1010	U.S. Provisional Application No. 62/209/221 to Beard, “Automatic Dependent Surveillance Broadcast Transmission within Whitespace,” filed August 24, 2015

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

1011	U.S. Patent No. 9,805,238 to Falk <i>et al.</i> , “System for Identifying and Controlling Unmanned Aerial Vehicles,” (“ <i>Falk</i> ”) filed July 11, 2016 and issued October 31, 2017
1012	U.S. Provisional Application No. 62/301,858 to <i>Falk</i> , “System for Identifying and Controlling Unmanned Aerial Vehicles,” (“ <i>Falk Provisional</i> ”), filed March 1, 2016
1013	Claim Listing of Challenged Claims
1014	Kayton, Myron and Fried, Walter, <i>Avionics Navigation Systems</i> , John Wiley and Sons, 1997.
1015	International Publication No. WO2016/154949 A1 to Gong <i>et al.</i> , “Authentication Systems and Methods for Generating Flight Regulations,” filed March 31, 2015 and published October 6, 2016
1016	International Publication No. WO2015/043123 A1 to Wang <i>et al.</i> , “Data Communication Systems and Methods,” filed January 14, 2014 and published April 2, 2015
1017	Burnside, Joseph E., “ADS-B Out: 978 UAT Or 1090ES?,” AviationSafety Magazine, published March 15, 2016.
1018	Nichols, Randall et al., <i>Counter Unmanned Aircraft Systems Technology and Operations</i> , New Prairie Press, 2020
1019	Austin, Reg, <i>Unmanned Aircraft Systems, UAVS Design, Development and Deployment</i> , Wiley, John Wiley and Sons, 2010
1020	Stipulation email on May 29, 2025
1021	Second Declaration of Dr. Girish Chowdhary
1022	International Publication No. WO2016/161637 to Gong et al., “Method, Apparatus and System of Providing Communication Coverage to an Unmanned Aerial Vehicle,” filed April 10, 2015 and published October 13, 2016 (“Gong637”)
1023	Transcript of Deposition of Dr. Nikolaos Papanikolopoulos
1024	Third Declaration of Dr. Girish Chowdhary
1025	U.S. Patent 9,087,451 to Jarrell, “Unmanned Aerial Vehicle Communication, Monitoring, and Traffic Management,” filed July 28, 2014, issued July 21, 2015 (“Jarrell”)
1026	U.S. Patent Application Publication No. 2016/0125740 to Pasko et al., “Unmanned Aerial Vehicle Identity and Capability Verification,” filed May 20, 2014, published May 5, 2016 (“Pasko”)

I. SCS 10-18 LACK WRITTEN DESCRIPTION SUPPORT

SC 10, [10.d]: PO's amendment to element [10.d] introduces an architectural contradiction that completely lacks written description support. EX1024, ¶¶42-43. Substitute Claim (SC) 10 recites, in part, *[a] discrimination system comprising: an identifier transmission system coupled to an unmanned aerial system . . . [and an] identification receiver [that] is configured to receive . . . a second identifier from a computer system that is remote relative to the discrimination system . . .* RMTA (Paper 25), 3-7 (emphasis added). The *identifier transmission system* is thus **part of** the *discrimination system*. *Id.* To prove written description support for the new requirement that the *second identifier* is received from a *computer system that is remote relative to the discrimination system*, PO must show the specification discloses the *second identifier* originating from somewhere *other than* the *identifier transmission system*. PO cannot meet this burden. The '303 Application provides only one source for the transmission of the *second identifier*: the *identifier transmission system* itself—which is, again, described and claimed as part of the *discrimination system*, not remote to it. EX2002, 2:18-22, 4:15-20 (“first and second identifier, transmitted by a first and second identifier transmission system.”); RMTA, 3. The “second identifier” is not described as being transmitted from anywhere other than an “identifier transmission system.” *Id.* And none of PO's cited disclosures provide sufficient support. RMTA, 6-8; EX1024, ¶¶44-45. PO appears

to primarily rely on two disclosures: a “second identifier, transmitted by a . . . second identifier transmission system” and a “dynamic aerial system identifier” that can be “generated remotely (e.g., at a remote computing system).” *Id.*; RMTA, 7-8 (citing EX2002, 4:15-20 and 14:23-15 [SIC]). However, as explained above, the first disclosure shows that the second identifier is transmitted by the “identifier transmission system” that is part of the *discrimination system*, not *remote* to it. EX2002, 4:15-20. And the second disclosure relates to the “aerial system identifier 310” that is recited elsewhere in the claim (the *first identifier*) and is not described as the claimed *second identifier*. EX2002, 14:23-15:7; *see also id.*, 6:1-3, 9:13-17, 14:6-17; RMTA, 3-5. Moreover, that the “dynamic aerial system identifier” can be **generated** remotely from the aerial system itself does not identify from where it is **transmitted** or from where the identification receiver **received** it. *Id.* And the context of the specification reveals that this “aerial system identifier 310” is transmitted from the “identifier transmission system 101”—which, again, is part of the discrimination system and not remote to the discrimination system. *Id.*, 15:15-16 (“identification transmitters of the identifier transmission system 101 functions to transmit the aerial system identifier 310.”), 6:1-3, 14:6-12. PO’s remaining citations relate to its other amendments and do not support receiving the *second identifier from a computing system that is remote relative to the discrimination system*. RMTA, 7-8 (citing EX2002, 8:16-9:1, 9:13-17, 30:17-18 and 30:24-31:1);

EX1024, ¶¶46-47. In short, PO’s amendment creates a fatal paradox. A component cannot be *remote relative to* the system it is a part of. Because the specification exclusively ties the transmission of the *second identifier* to the *identifier transmission system* that is claimed as part of the *discrimination system*, PO cannot show possession of an architecture where that transmission originates *remote to* the *discrimination system*. SC 10 is not supported; dependent SCs 11-18 are also thus unsupported. *Id.* **SC 10, [10.e2]:** [10.e2] recites *to provide the authenticated first identifier...to the permission module*, but this is unsupported. RMTA, 9; EX2002, 4:15-5:1, 30:16-31:8, EX1024, ¶¶48-49. The specification describes “raw or processed” signals, decrypted signals, and verification of identifier 310, but none of this discloses an *authenticated first identifier* is ***provided*** to a permission module. EX2002, 2:18-20, 9:13-23, 3:8-10, 8:21-23, 18:7-19:21, 30:16-31:8, 32:19-36:2, Figs. 1, 6; EX1024, ¶¶49-50. SC 10 lacks support; SCs 11-18 thus do as well. *Id.*

II. THE SCS ARE UNPATENTABLE

A. SCs 10-18 are Indefinite

1. Independent SC 10: [10.d]

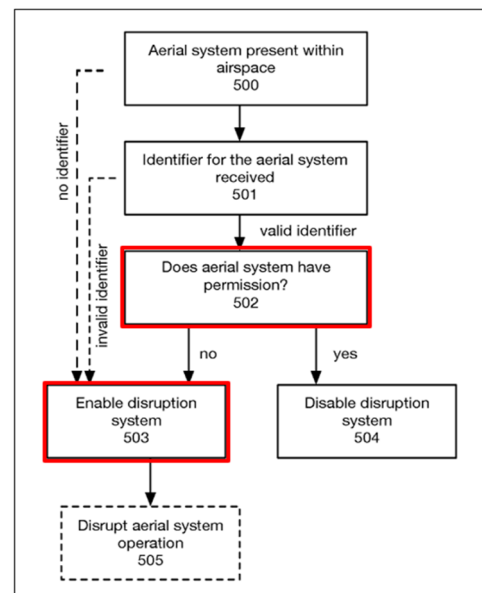
“[A] computing system remote relative to the discrimination system” creates an irreconcilable contradiction that renders the SCs indefinite and precludes a POSITA from determining the claim’s scope with reasonable certainty. EX1024, ¶¶51-52. Courts have held claims indefinite where they are logically inconsistent such that a POSITA cannot understand their boundaries. *Trustees of Columbia University in the*

City of New York v. Symantec Corp., 811 F.3d 1359 1366-67 (Fed. Cir. 2016); *Competitive Technologies, Inc. v. Fujitsu Ltd.*, 185 F. App'x 958, 965-66 (Fed. Cir. 2006). So too here. SC 10 recites a *discrimination system* that includes an *identifier transmission system*. RMTA, 3. Later, SC 10 requires an *identification receiver* configured to receive a *second identifier functioning as a second factor identifier* from a computing system that is “***remote relative to the discrimination system.***” *Id.*, 6-7. But the **only** source of the *second identifier functioning as a second factor identifier* is the identifier transmission system. Section I ([10.d]). If the identifier transmission system is the source of the identifier, it cannot logically be *remote relative to* the very discrimination system of which it is a claimed part. A system cannot be remote from itself. As a POSITA is left to guess to how to resolve this inconsistency, SC 10 and dependent SCs 11-18 are indefinite. EX1024, ¶52.

2. Independent SC 10: Element [10.g]

Element [10.g] recites “*wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.*” RMTA, 10-13. The intrinsic record does not provide any insight into the meaning of “*preemptively enabled,*” making SC 10’s scope ambiguous and unclear. EX1024, ¶¶53-55. The specification does not differentiate between the meaning of “*preemptively enabled*” and “*enabled,*” which sows uncertainty into SC 10 and provides the claim language has several different meanings. *Id.*; *Interval Licensing v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014).

Thus, the Petition addressed “preemptively enabled” under multiple possible interpretations. Pet., 25-27, 44-47, 63-65. The patent’s only reference to “*preemptively enabled*” is “certain scenarios may require the disruption system 105 to be ready to engage on short notice” and “[a]s depicted in FIG. 5, the disruption system 105 may thus be preemptively enabled if certain conditions are met (e.g. aerial system detected w/o an identifier 500, identifier is received but is invalid 501, identifier is valid but is not permissioned 502, etc.).” EX1001, 19:14-25 (emphasis added) (parenthetical in original). Figure 5 shows the three “conditions” 500, 501, and 502 that the specification says cause disruption system 105 to be “*preemptively enabled*.” EX1001, Fig. 5. But for condition 502 (“identifier is valid but is not permissioned”), the disruption system goes directly to being “enable[d]” at step 503 and does not show anything that is “*preemptively enabled*.” EX1001, Fig. 5; EX1024, ¶¶55-56. This contrasts with condition 500 that, if there is no identifier, enables the disruption system preemptively—without checking conditions 501 and 502. EX1001, Fig. 5. This also contrasts with condition 501 that, if there is an invalid identifier, enables the system preemptively—without checking condition 502.



EX1001, Fig. 5. The specification is thus unclear on if “*preemptively enabled*” is the

same or different to “enabled.” EX1024, ¶57; EX1023, 80:2-15, 84:21-85:1 (PO’s expert equating “preemptively enabled” to “activate.”). The multiple potential meanings and specification’s missing guidance on which is correct renders SC 10 indefinite. EX1024, ¶57-59. Dependent SCs 11-18 are also thus indefinite. **SC 18** is also indefinite as no antecedent basis for *the control system*. *Id.*; RMTA, 3-13, 18.

B. SCs 10-18 Are Obvious

Petitioners address the SC limitations added in the RMTA and relevant original claim limitations; unaddressed original claim limitations are addressed in the Pet. Indefinite and/or lacking written description elements are addressed based on Petitioners’ understanding of PO’s position and as best understood by a POSITA.

GND	SC(s)	Basis	Prior Art
7B/7C	10-12, 14-18	103	Whitmarsh, Jarrell, Gong637 (7B)/ Whitmarsh, Jarrell, Gong637, Pasko (7C)
8B/8C	13	103	Whitmarsh, Falk, Jarrell, Gong637 (8B)/ Whitmarsh, Falk, Jarrell, Gong637, Pasko (8C)
9B/9C	10-12, 14-18	103	Whitmarsh, Goodrich, Jarrell, Gong637 (9B)/ Whitmarsh, Goodrich, Jarrell, Gong637, Pasko (9B)
10B/10C	13	103	Whitmarsh, Goodrich, Falk, Jarrell, Gong637 (10B)/ Whitmarsh, Goodrich, Falk, Jarrell, Gong637, Pasko (10C)
11	10-12, 14-18	103	Whitmarsh, Viggiano, and Gong637
12	13	103	Whitmarsh, Falk, Viggiano, and Gong637
13	10-12, 14-18	103	Whitmarsh, Goodrich, Viggiano, and Gong637
14	13	103	Whitmarsh, Goodrich, Falk, Viggiano, and Gong637

Grounds 7B-10B/7C-10C rely on original grounds 1-4 from the Petition and add Jarrell (EX1025) and Gong637 (EX1022), and Pasko (EX1026) (for 7C-10C).

Grounds 11-14 rely on original grounds 1-4 from the Petition and add Viggiano (EX1007) and Gong637. Jarrell (filed July 28, 2014, issued July 21, 2015), Gong637 (filed April 10, 2015), and Pasko (filed May 20, 2014) are each prior art to the SCs under 35 U.S.C. § 102(a)(2), and Jarrell is further 102(a)(1) prior art, as of the '199 Patent's earliest claimed priority date of March 17, 2016. EX1025, Cover Page; EX1022, Cover Page; EX1026, Cover Page; EX1001, Cover Page. Jarrell, Gong637, and Pasko are each in the same field of art as the '199 Patent and describe aircraft authentication similar to the '199 Patent. EX1025, Abstract, 1:14-17, 13:23-14:14; EX1022, ¶¶0094, 0122; EX1001, Abstract, 2:10-15; EX1026, Abstract, ¶¶0020, 0035-0042; EX1024, ¶¶60-71. Gong637 is different from U.S. Patent No. 9,792,613 to Gong listed on the face of the 199 Patent. EX1001, Cover Page. Viggiano is prior art to the '199 Patent and in its same field of art. Petition (Paper 13, "Pet."), 8.

1. Grounds (GNDs) 7B/7C and 9B/9C: SCs 10-12 and 14-18

Motivation to Combine (MTC) 1: A POSITA would have been motivated to combine Whitmarsh, Jarrell, and Gong637 (GND 7B) and to combine Whitmarsh, Goodrich, Jarrell, and Gong637 (GND 9B). Pet., 40-44; EX1024, ¶72. Jarrell is directed to techniques to "authenticate or validate the registration or license identifier of [] [a] UAV." EX1025, 13:23-14:15. A UAV transmits its identifier to a "communications station 101." *Id.* The communications station 101 communicates with a "control center 148 remote from the communications station 101, to

authenticate or validate” the identifier of the UAV. *Id.* The control center 148 “provide[s] a list, and the communications station 101 may compare the UAV registration or license identifier to the list and make a determination regarding the UAV’s compliance.” *Id.* If the UAV fails this comparison and has an invalid registration or license identifier (i.e., not authenticated), the communications station 101 transmits a message to a “police department” or “civil airspace authority” to inform them of the invalid registration or license. *Id.* Gong637 discloses UAV aircraft authentication in which a UAV “may be authenticated through the entire flight path.” EX1022, ¶¶0094, 0122. UAV identification can be “authenticated by checking and confirming the identification with an authentication center on the communication network.” *Id.* Failed authentication results in the UAV being “forced to land.” *Id.* UAV systems were known to present “unauthorized or intrusive surveillance opportunities that could arise as unmanned aerial vehicles become more prevalent.” EX1025, 1:44-47; EX1024, ¶¶72-74. Another known problem in UAV systems was “spoofing” or fraudulent UAV identities. EX1007, ¶¶0003-0004; EX1025, 13:23-14:15; EX1024, ¶74. Bad actors using such techniques could gain access to unauthorized airspace. *Id.* As Jarrell and Gong637 are highly relevant to addressing such known problems, a POSITA would have made the combinations. EX1024, ¶74. Whitmarsh, as well as Whitmarsh and Goodrich, teach using a UAV MAC address to identify a UAV, and Jarrell and Gong637 provide enhancements by

teaching identification techniques as discussed above that help ensure such a UAV MAC address is authentic and not fraudulent. *Id.*; EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0017; Pet., 18-19; EX1025, 13:23-14:15; EX1022, ¶¶0094, 0122. The combinations would have provided that a received UAV MAC address is authenticated, by Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses, by checking the address against a list received from a remote center—thus verifying an authenticity of the UAV MAC address—and that the UAV is forced to land if authentication fails (i.e., authenticity of the MAC address of the UAV has not been verified). EX1025, 13:23-14:15; EX1022, ¶¶0094, 0122; EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0018, pp. 22-25; EX1024, ¶¶74-75; Pet., 16-25, 44. After successful authentication, an authenticated UAV MAC address would have then been usable by the combinations' systems, which would have been a benefit by ensuring that the MAC address is valid. *Id.* The combination would have thus used known authentication techniques that were straightforward to implement and thus would have had predictable results with a reasonable expectation of success. *Id.*

MTC2: A POSITA would have been further motivated to combine Whitmarsh, Jarrell, and Gong637 with Pasko (GND 7C) and to combine Whitmarsh, Goodrich, Jarrell, and Gong637 with Pasko (GND 9C). EX1024, ¶76. Pasko discloses techniques for authenticating UAVs, and is thus highly relevant to solving the same

known problems noted in MTC1. *Id.*; EX1026, Abstract, ¶¶0035-0042; Section II.B.1, *supra*. In Pasko, a UAV transmits “credentials,” that include an “identification number,” “serial number,” and “government registration number”—all associated with the UAV—to a computing platform 230. EX1026, Abstract, ¶¶0010, 0020, 0022, 0026, 0035-0042. The platform then uses “account information” from a distributed (i.e., remote) database 235 to authenticate the UAV (and its associated credentials) by comparing the received credentials and received account information. *Id.* The account information includes “information associated with authenticated and registered UAVs” such as “identification numbers of UAVs,” “public and/or private keys of UAVs,” and “account status” of UAVs, as well as a government registration number. *Id.*, ¶¶0037-0038. The computing platform authenticates the UAV by comparing the serial number and government registration number of the UAV credentials against received identification information and a government registration number of the account information, to determine whether the UAV is registered with the computing platform, an account associated with the UAV is in good standing, and the UAV is “registered with the appropriate authority.” *Id.* An authenticity of the UAV’s serial number is verified as the serial number is associated with a properly registered UAV and good standing account through the comparisons. *Id.* Moreover, an authenticity of the UAV’s serial number is verified as the serial number is associated with a UAV that is properly registered

with a government authority. *Id.*; EX1024, ¶76. A POSITA would have combined Pasko's teachings with Whitmarsh, Jarrell, and Gong637 (GND 7C)/ Whitmarsh, Goodrich, Jarrell, and Gong637 (GND 9C) such that Pasko's remotely stored account information (including identification information and government registration number) is present at Jarrell's remote control center, where Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (1) receives credentials including the identifier UAV MAC address and government registration number from a UAV, (2) receives the account information from Jarrell's remote control center, and (3) authenticates a received UAV MAC using the account information, comparing the UAV MAC address and government registration number of the UAV credentials against identification information and a government registration number of the account information. EX1026, Abstract, ¶¶0010, 0020, 0022, 0026, 0035-0042; EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0018, pp. 22-25; Pet., 16-25, 44; EX1024, ¶77. After successful authentication, an authenticated UAV MAC address would have then been usable by the combinations' systems, which would have benefitted the systems by ensuring that the MAC address is valid. *Id.* The combinations would have provided the same benefits as those discussed above for MTC1 (Section II.B.1, *supra*), and would have improved system security, providing an additional layer of authentication through verification of additional information

(e.g., government registration number). EX1026, ¶0008; EX1024, ¶77. The combination would have been easily implementable because it simply involves storing additional data in a remote database and performing authentication using such data, which is predictable. Section II.B.1, *supra*; EX1024, ¶77. The combination thus would have had a reasonable expectation of success. *Id.* **SC 10:** **[10.a]:** Whitmarsh discloses a transmission system coupled to an unmanned aerial vehicle (UAV) (*an identifier transmission system coupled to an unmanned aerial system*). EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0017; Pet, 16-18, 44; EX1024, ¶78. Whitmarsh discloses wireless communications transmitted by the UAVs transmission system comprise information or signatures unique to the UAV, such as a MAC address of the UAV, that is used to identify the transmitting UAV (*the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system*). *Id.* **[10.b]:** Whitmarsh’s UAV defense system would have included an *identification receiver* for the reasons discussed in the Petition. EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0017; EX1024, ¶79; Pet., 16-25, 44. The UAV defense system can “identify the UAVs 14 by passive means, i.e., by simply detecting radio signals 54” and “by capturing the MAC address, which is unique to each UAV 14, the UAV defense system 10 will be able to specifically identify the detected UAV 14.” EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0018, pp. 22-25.

Due to this functionality, a POSITA would have thus understood, or at least found obvious, that Whitmarsh's UAV defense system comprises a computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*identification system*), and that the computer system, processor, or similar component would have further included the parts forming an *identification receiver* that receives wireless communications and identification information (e.g., the MAC addresses) contained therein that is transmitted by UAVs (*identification system comprising an identification receiver*). *Id.*; EX1024, ¶79; Pet., 16-25, 44. **[10.d]: GND7B/9B:** The combinations teach Whitmarsh's parts forming the *identification receiver* would have received (1) the wireless communications that include information or signatures unique to the UAV, such as the MAC address of the UAV, from the UAV (*wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system*) as well as (2) a list of valid MAC address identifiers that includes a valid MAC address identifier relevant to the UAV, received from a remote control center (*and (ii) a second identifier from a computing system that is remote relative to the discrimination system*). EX1025, 10:53-59, 11:49-55, 12:12-17, 12:47-65, 13:23-14:15, 18:31-35, 25:13-47; Sections II.B.1 (MTC1, [10.a], [10.b]); Pet., 16-25, 44; EX1024, ¶80. As combined, Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses

(*identification system*) “compare[s]” the MAC address of the UAV to the list of valid MAC address identifiers, where a match between the MAC address of the UAV and the valid MAC address identifier relevant to the UAV (*the second identifier*) located on the list “authenticate[s]” the MAC address of the UAV. *Id.*; see also EX1025, 13:23-59; Section II.B.1 (MTC1); EX1024, ¶80. Thus, the valid MAC address identifier relevant to the UAV of the list (*the second identifier*) is *functioning as a second factor identifier* for the UAV (*for the unmanned aerial system*) because it is a second identifier to the UAV’s transmitted MAC address that authenticates the transmitted MAC address and determines whether the UAV is compliant. *Id.*

GND7C/9C: The analysis for GND7C/9C is the same as for 7B/9B, except that the (ii) *a second identifier from a computing system that is remote relative to the discrimination system* is formed by account information (e.g., government registration number) received from Jarrell’s remote control center, which is used by Whitmarsh’s computer system, processor, or similar component that identifies UAVs (*identification system*) to authenticate the received UAV MAC (*first identifier*). Section II.B.1 (MTC2); EX1024, ¶80. In the GND7C/9C combinations, Whitmarsh’s computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (1) receives credentials including the identifier UAV MAC address and government registration number from a UAV, (2) receives the account information from Jarrell’s remote control center, and (3)

authenticates a received UAV MAC using the account information, comparing the UAV MAC address and government registration number of the UAV credentials against identification information and a government registration number of the received account information. EX1026, Abstract, ¶¶0010, 0020, 0022, 0026, 0035-0042; EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0018, pp. 22-25; Pet., 16-25, 44; Section II.B.1 (MTC2); EX1024, ¶80. An authenticity of the UAV's MAC address is verified as the MAC address is associated with a properly government registered UAV and good standing account through the authentication comparisons. *Id.* Moreover, an authenticity of the UAV's MAC address is further verified as the MAC address is associated with a UAV that is properly registered with a government authority. *Id.* The received account information (*the second identifier*) is *functioning as a second factor identifier* for the UAV (*for the unmanned aerial system*) because it is a second identifier (including UAV identification number, UAV public/private keys, UAV account status, and government registration number) to the UAV's transmitted MAC address that authenticates the MAC address. *Id.* The account information is also a different piece of information (e.g., a government registration number) from the UAV MAC address that is used in an additional comparison (e.g., using government registration numbers), which further provides the account information (*the second identifier*) is *functioning as a second factor identifier* for the UAV (*for the unmanned aerial system*). *Id.* **[10.e1]:**

Whitmarsh’s computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*the identification system*) uses the parts forming an *identification receiver* to receive wireless communications and identification information (e.g., the MAC addresses) contained therein that is transmitted by UAVs. Section II.B.1 ([10.b]). As combined, a POSITA would have understood or at least found obvious that Whitmarsh’s computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*the identification system*) would have been configured to determine the MAC address of the UAV from the wireless communications (*is configured to determine the first identifier from the aerial system identifier signal*). *Id.*; EX1024, ¶81. This is because the combination teaches that Whitmarsh’s computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*the identification system*) performs authentication of the UAV’s received MAC address, and would have thus deciphered the MAC address from the wireless communications. *Id.*; Section II.B.1 ([10.d], MTC1); EX1025, 22:19-52. Moreover, for **GND7B/9B**, as discussed in Section II.B.1 ([10.d]), Whitmarsh’s computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*the identification system*) “compare[s]” the MAC address of the UAV (*first identifier*) to the list of valid MAC address identifiers to perform authentication and thus check an authenticity of the MAC address of the UAV

(*verify an authenticity of the first identifier*), where a match between the MAC address of the UAV (*first identifier*) and the valid MAC address identifier relevant to the UAV (*the second identifier*) located on the list “authenticate[s]” the MAC address of the UAV (*verify an authenticity of the first identifier using the second identifier*). Pet., 16-25, 44; EX1024, ¶81. For **GND7C/9C**, the analysis is the same as for 7B/9B, except that *the second identifier* is formed by account information from Jarrell’s remote control center, which is used by Whitmarsh’s computer system, processor, or similar component that identifies UAVs (*identification system*) to authenticate the received UAV MAC address (*verify an authenticity of the first identifier using the second identifier*), verifying an authenticity of the UAV’s MAC address as the MAC address is associated with a properly government registered UAV and good standing account through the authentication comparisons, and further verifying an authenticity of the UAV’s MAC address as the MAC address is associated with a UAV that is properly registered with a government authority. Section II.B.1 (MTC1); EX1024, ¶81. For all grounds, successful authentication would have resulted in Whitmarsh’s UAV MAC address having been authenticated, and thus provided an authenticated UAV MAC address (*and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified*). Section II.B.1 (MTC1, MTC2); Section II.B.1 ([10.d]); Pet., 16-25, 44; EX1024, ¶81. **[10.e2]:** The combination teaches that

successful authentication would have resulted in Whitmarsh's authenticated UAV MAC address provided to the *permission module (to provide the authenticated first identifier of the aerial system identifier signal to the permission module)*. Sections II.B.1 (MTC, [10.e1]); Pet., 19-20, 44; EX1024, ¶82. **[10.f]:** The combinations teach the components forming the *permission module* would have determined that a UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace*). *Id.*; Sections II.B.1 (MTC1, [10.e1], [10.e2]); Pet., 21-25, 44; EX1024, ¶83. **[10.g]:** The combinations teach a disruption of the detected UAV provided by a countermeasures system would have occurred when the components forming the *permission module* determine that the UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in an airspace*). Pet., 21-27, 44-47; EX1005, ¶¶0017, 0018, 0028, 0029; EX1006, ¶¶0009-0011, 0013, 0016-0018; Section II.B.1 (MTC1, MTC2, [10.d], [10.e1], [10.e2]); EX1024, ¶84. The combinations further teach that Whitmarsh's countermeasures system (*disruption system*) disrupts operation of the

UAV by forcing it to land (*configured to disrupt an operation of the unmanned aerial system*) when the authentication of the UAV's MAC address fails and authenticity of the UAV's MAC address is not verified ((*ii*) *when the authenticity of the first identifier is not verified*). *Id.* The combinations further teach *wherein the disruption system is preemptively enabled based on the received aerial system identifier signal* as discussed in the Pet. at 25-27, 44-47. **SCs 11-12 and 14-18:** Taught as in the Pet. for orig. claims 2-3 and 5-9. Pet., 27-35, 47-51. EX1024, ¶85.

2. GNDs 8B/8C and 10B/10C

GNDs 8B/8C and 10B/10C teach SC 13 for the reasons of the Pet. at 35-40, 51 for original claim 4. A POSITA would have been motivated to combine Jarrell and Gong637, and Jarrell, Gong637, and Pasko, with Whitmarsh and Falk/Whitmarsh, Goodrich, and Falk for the Section II.B.1 (MTC) reasons. EX1024, ¶86.

3. GNDs 11 and 13

MTC: A POSITA would have been motivated to combine Whitmarsh, Viggiano, and Gong637 (GND 11), and to combine Whitmarsh, Goodrich, Viggiano, and Gong637 (GND 13). Pet., 40-44; EX1024, ¶87. Viggiano is directed to aircraft identity authentication techniques using multiple forms of aircraft identification. EX1007, ¶¶0004, 0006-0007, 0011-0024, Figs. 1-3. An authenticator receives, from an aircraft, identification information 32 and a message authentication code (AC) 38 that is formed from identification information 22 and a secret key 36 unique to the

aircraft. *Id.* At the authenticator, another message AC 58 is formed using the received identification information 32. *Id.* A comparator compares the message AC 58 and message AC 38, and a match that results from the comparison indicates that the transmitting aircraft's identity (and thus identification information 32 and 22) is authenticated, verifying an authenticity of the identity. *Id.*, ¶¶0015. Failed comparisons (i.e., no match) results in a "responsible higher command authority" being notified so they can "respond appropriately." *Id.* Gong637 discloses UAV identification can be "authenticated by checking and confirming the identification with an authentication center on the communication network." EX1022, ¶¶0094, 0122. Failed authentication results in the UAV being "forced to land." *Id.* Gong637 further discloses that its UAV transmits data using a first communication unit (dedicated communication unit 426) and a second communication unit (public communication unit 428), where the communications from each unit are receivable by a terminal having two communication units that receive data from the UAV's first communication unit and second communication unit, respectively. EX1022, ¶¶0087-0098. A known problem in UAV systems was "spoofing" or fraudulent UAV identities. EX1007, ¶¶0003-0004; EX1024, ¶¶87-88. Bad actors using such techniques could gain access to unauthorized airspace. *Id.* As Viggiano and Gong637 are highly relevant to addressing such known problems, a POSITA thus would have formed the combinations. EX1024, ¶88. Whitmarsh, as well as

Whitmarsh and Goodrich, teach using a UAV MAC address to identify a UAV, and Viggiano and Gong637 provide enhancements by teaching identification authorization techniques as discussed above that would help ensure such a UAV MAC address is properly authenticated. *Id.*; EX1005, ¶¶0020, 0027; EX1006, ¶¶0008, 0010, 0013, 0015-0017; Pet., 18-19; EX1007, ¶¶0004, 0006-0007, 0011-0024, Figs. 1-3; EX1022, ¶¶0094, 0122. Gong637 further teaches basic and well-known communication techniques of using separate communication units for different transmissions. EX1022, ¶¶0087-0098; EX1024, ¶88. The combinations would have thus provided that Whitmarsh's component for receiving wireless communications and the identification information would have received (1) UAV aircraft identification information that is the wireless communication signal including the MAC address of a UAV, from a first communication unit of the UAV, as well as (2) a message AC formed from identification information of the UAV and a secret key of the UAV, from a second communication unit of the UAV. Sections II.B.3 ([10.a], [10.b]), II.B.1 ([10.a], [10.b]); EX1007, ¶¶0004, 0006-0007, 0011-0024, Figs. 1-3; EX1022, ¶¶0087-0098, 0122; Pet., 16-25, 44; EX1024, ¶89. Moreover, Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses would have verified an authenticity of the received UAV MAC address by (1) forming a first message AC using the received UAV MAC address and (2) comparing the first message AC to

the received message AC, where a match that results indicates the UAV's MAC address (identity) is verified and no match indicates authenticity is not verified—with Whitmarsh's countermeasures system disrupting operation of the UAV in such a case by forcing it to land. EX1007, ¶¶0004, 0006-0007, 0011-0024, Figs. 1-3; EX1022, ¶¶0094, 0122; Sections II.G.2.a-c ([10.a], [10.b], [10.d]); Pet., 16-25, 44; EX1024, ¶89. After successful authentication, an authenticated UAV MAC address would have then been usable by the combinations' systems, benefitting the systems by ensuring the MAC address is not fraudulent. *Id.* The combinations represent application of known techniques (known aircraft identification authentication and communication techniques) to a known system (Whitmarsh/Whitmarsh and Goodrich systems) ready for improvement; the results would have been predictable with a reasonable expectation of success. *Id.* **SC 10: [10.a], [10.b]:** Sections II.B.1 ([10.a], [10.b]). **[10.d]:** Whitmarsh's parts forming an *identification receiver* would have received (1) UAV aircraft identification information that is the wireless communication signal including the MAC address of a UAV, from a first communication unit of the UAV (*wherein the identification receiver is configured to receive (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system*), as well as (2) a message AC formed from identification information of the UAV and a secret key of the UAV, from a second communication unit of the UAV (*and (ii) a second identifier from a computing system that is remote*

relative to the discrimination system). Sections II.B.3 (MTC, [10.a], [10.b]); EX1007, ¶¶0004, 0006-0007, 0011-0028, Figs. 1-3; EX1022, ¶¶0087-0098, 0122; Pet., 16-25, 44; EX1024, ¶¶90-94. The message AC (*the second identifier*) is functioning as a second factor identifier for the unmanned aerial system as it is formed from identification information and a unique secret key of the UAV, is a second piece of identification information that is received (the first piece of identification information is the MAC address of the UAV), and is used to authenticate the UAV aircraft's identity. *Id.*; EX1007, ¶¶0004, 0006-0007, 0011-0027, Figs. 1-3, claims 1-4, 8-11, 17, 19. **[10.e1]**: The combinations teach Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*identification system*) would have verified an authenticity of the UAV's MAC address by (1) forming a first message AC using the received UAV MAC address and (2) comparing the first message AC to the received message AC, where a match indicates the UAV's MAC address (identity) is verified (*configured to...verify an authenticity of the first identifier using the second identifier*). EX1007, ¶¶0004, 0006-0007, 0011-0024, Figs. 1-3; EX1022, ¶¶0094, 0122; Sections II.B.3 (MTC, [10.a], [10.b], [10.d]); Pet., 16-25, 44; EX1024, ¶¶95-96. As Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*the identification system*) forms the first message AC using the received UAV MAC

address, a POSITA would have understood or at least found obvious that Whitmarsh's computer system, processor, or similar component (*the identification system*) would have deciphered the received MAC address from the wireless communications it was contained in (*is configured to determine the first identifier from the aerial system identifier signal*). *Id.*; EX1024, ¶96. Successful authentication would have resulted in Whitmarsh's UAV MAC address having been authenticated and thus provided by Whitmarsh's *identification system* an authenticated UAV MAC address (*to provide an authenticated aerial system identifier of the aerial system identifier signal when the authenticity has been determined and verified*). *Id.* **[10.e2]:** The combinations would have provided the authenticated UAV MAC address to the components forming the *permission module* (*to provide the authenticated aerial system identifier of the aerial system identifier signal to the permission module*). Pet., 19-20, 44; Sections II.B.3 (MTC, [10.d], [10.e1]); EX1024, ¶97. **[10.f]:** Successful authentication results in an authenticated UAV MAC address; the components forming the *permission module* would determine a UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace*). Pet., 21-25, 44; Sections II.B.3 (MTC, [10.d], [10.e1], [10.e2]); EX1024, ¶98. **[10.g]:** The combinations teach a

countermeasures system disrupts detected UAV operation when the components forming the *permission module* determine the UAV associated with the authenticated UAV MAC address is not authorized for a particular area (*a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in an airspace*). Pet., 21-27, 44-47; EX1005, ¶¶0017, 0018, 0028, 0029; EX1006, ¶¶0009-0011, 0013, 0016-0018; EX1024, ¶99. The countermeasures system (*disruption system*) disrupts the UAV's operation by forcing it to land (*configured to disrupt an operation of the unmanned aerial system*) when the authentication comparison involving the UAV MAC address fails and authenticity of the UAV's MAC address is not verified (*(ii) when the authenticity of the first identifier is not verified*). Section II.B.3 (MTC, [10.d], [10.e1]); EX1007, ¶0015; EX1024, ¶100. The combinations teach *wherein the disruption system is preemptively enabled based on the received aerial system identifier signal* as discussed in the Pet. at 25-27, 44-47. *Id.* **SCs 11-12 and 14-18**: Taught as in the Pet. for orig. claims 2-3 and 5-9. Pet., 27-35, 47-51. EX1024, ¶101.

4. GNDs 12 and 14

GNDs 12 and 14 teach SC 13 as in the Pet. at 35-40, 51 for orig. clm. 4. A POSITA would have been motivated to combine Viggiano and Gong637 with Whitmarsh and Falk/Whitmarsh, Goodrich, and Falk for the II.B.3 (MTC) reasons. EX1024, ¶102.

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 1024-1026** 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