

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

**DECLARATION OF DR. GIRISH CHOWDHARY IN SUPPORT OF
PETITIONERS' OPPOSITION TO PATENT OWNER'S NON-
CONTINGENT MOTION TO AMEND**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. EXPERIENCE AND QUALIFICATIONS.....	1
III. TASK SUMMARY AND MATERIALS REVIEWED	1
IV. LIST OF EXHIBITS.....	2
V. TECHNICAL BACKGROUND	5
VI. OVERVIEW OF THE CHALLENGED PATENT.....	5
VII. LEGAL STANDARDS	5
VIII. OVERVIEW OF THE SUBSTITUTE CLAIMS.....	7
A. Table Correlating Original Claim to Substitute Claim	7
B. List of Substitute Claim.....	7
IX. PRIORITY DATE OF THE SUBSTITUTE CLAIM	9
X. CLAIM CONSTRUCTION	9
XI. SUMMARY OF CONCLUSIONS AND GROUNDS FOR CHALLENGE	10
XII. THE SUBSTITUTE CLAIM ENLARGES CLAIM SCOPE	12
XIII. THE SUBSTITUTE CLAIM LACKS WRITTEN DESCRIPTION SUPPORT.....	12
A. Substitute Claim 22: Element [22.i].....	12
B. Substitute Claim 22: Element [22.e]	17
XIV. THE SUBSTITUTE CLAIM IS INDEFINITE.....	20
A. Substitute Claim 22: Element [22.c]	20
XV. THE SUBSTITUTE CLAIM IS OBVIOUS	22
A. Overview of <i>Viggiano</i> (Ex. 1024).....	23
B. Overview of <i>Byers</i> (Ex. 1025).....	24
C. Ground 5: Beard and Viggiano	27
D. Grounds 6 and 7: Taveira, Wang, Gong, and Viggiano (Ground 6)/Taveira, Qi, Gong, and Viggiano (Ground 7).....	33
E. Ground 8: Gong, Wang-II, and Viggiano	35

F.	Ground 9: Beard and Byers	38
G.	Grounds 10 and 11: Taveira, Wang, Gong, and Byers (Ground 10)/Taveira, Qi, Gong, and Byers (Ground 11)	44
H.	Ground 12: Gong, Wang-II, and Byers	46
XVI.	CONCLUSION.....	48

Second Declaration of Dr. Girish Chowdhary

I. INTRODUCTION

1. My name is Dr. Girish Chowdhary. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters contained herein.

2. I had previously authored and then signed a declaration on January 28, 2025, which I understand was submitted as Exhibit 1003 to the Patent Trial and Appeal Board (“PTAB”) of the United States Patent and Trademark Office in case number IPR2025-00525. I may alternatively refer to the January 28, 2025, declaration as “Exhibit 1003” or “Original Declaration.”

3. In this Second Declaration, I incorporate the facts and opinions outlined in my Original Declaration.

II. EXPERIENCE AND QUALIFICATIONS

4. My experience, qualifications, CV, and consulting fee are outlined in my Original Declaration.

III. TASK SUMMARY AND MATERIALS REVIEWED

5. My Original Declaration addressed U.S. Patent No. 10,713,959 (Ex. 1001, “’959 Patent”).

6. I have been informed that Airspace Defense, Inc. (“Patent Owner” or “PO”) submitted Non-Contingent Motion to Amend for the ’959 Patent (Paper 16, “Motion to Amend” or “MTA”) in case number IPR2025-00525 on December 20,

2025, in which it has proposed a “Substitute Claim” 22 to replace “Original Claim” 21 of the ’959 Patent. Counsel has informed me that the Motion to Amend was filed as “non-contingent,” which I understand means that the Board will issue a final decision on the patentability of the Substitute Claim rather than determining the patentability of the corresponding Original Claim.

7. I have been asked to review the MTA filed by PO regarding the ’959 Patent, the proposed Substitute Claim, and the exhibits cited by PO. I have been asked to provide an understanding of the technology relevant to the MTA, to review certain prior-art references, and analyze whether or not those references disclose or teach limitations of the proposed Substitute Claims. The opinions stated in this declaration are from the perspective of a person of ordinary skill in the art (“POSITA”).

IV. LIST OF EXHIBITS

8. In forming my opinions, I have reviewed the ’959 Patent, its prosecution history and references cited by the Examiner, the materials cited in the List of Exhibits, and the materials cited throughout my Original Declaration, and this declaration.

Ex.	Description
-----	-------------

No. ¹	
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),” (“Beard”) filed February 26, 2018 and issued August 4, 2020
1009	U.S. Provisional Application No. 62/480,031 to Beard, “Remote Identification” (“Beard Provisional”), filed March 31, 2017
1010	U.S. Patent Application Publication No. 2016/0253907 to Taveira, “Systems and Method for Restricting Drone Airspace Access,” (“Taveira”) filed January 29, 2015 and published September 1, 2016

¹ Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to Exhibit 1002, 1007, and 106 are made with reference to the Bates-stamped pagination; citations to other exhibits are made to the page number of the document itself.

1011	International Publication No. WO2016/078093 A1 to Wang <i>et al.</i> , “System and Methods for Managing Unmanned Aerial Vehicles,” (“Wang”) filed November 21, 2014 and published May 26, 2016
1012	International Publication No. WO2016/154949 A1 to Gong <i>et al.</i> , “Authentication Systems and Methods for Generating Flight Regulations,” (“Gong”) filed March 31, 2015 and published October 6, 2016
1013	U.S. Patent Application Publication No. 2016/0127890 to Qi <i>et al.</i> , “Apparatus, System and Method of Protecting a Service Identifier,” (“Qi”) filed December 24, 2014 and published May 5, 2016
1014	International Publication No. WO2015/043123 A1 to Wang <i>et al.</i> , “Data Communication Systems and Methods,” (“Wang-IP”) 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 Liu <i>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

1024	U.S. Patent Application Publication 2007/0239986 to Viggiano <i>et al.</i> , “Secure ADS-B Authentication System and Method,” (“Viggiano”) filed April 7, 2006 and published October 11, 2007
1025	U.S. Patent No. 9,875,660 to Byers <i>et al.</i> , “Multi-Modal UAV Certification,” (“Byers”) filed March 28, 2016 and issued January 23, 2018
1026	Transcript of Deposition of Dr. Nikolaos Papanikolopoulos

V. TECHNICAL BACKGROUND

9. See Section IX of my Original Declaration (Ex. 1003) for a technology background pertinent to the ’959 Patent.

VI. OVERVIEW OF THE CHALLENGED PATENT

10. See Section VI of my Original Declaration (Ex. 1003) for an overview of the ’959 Patent.

VII. LEGAL STANDARDS

11. The Legal Standards provided to me were described in my Original Declaration.²

12. In addition to those legal standards, I have been informed by counsel as to a legal background on indefiniteness. I have been informed that, in order to be valid, the claims of a patent must be sufficiently definite that one skilled in the art can determine the metes and bounds of the claimed invention. I have been informed that a patent claim is deemed “indefinite” if the claim, read in light of the patent’s

² EX1003 (Original Declaration), § V.

specification and prosecution history, fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. I understand that a claim must be precise enough to afford clear notice of what is claimed, thereby apprising the public of what is still open to them.

13. In addition to these legal standards, I have been informed by counsel as to the legal background on lack of written description. I have been informed that, in order for claims to be valid, the claims of a patent must provide written description support for each limitation of the claims. I have been informed that a patent claim lacks written description if the specification fails to convey with reasonable clarity to a POSITA that the inventor was in possession of the invention as of the filing date sought. I have been informed that this requirement relies on an objective inquiry into what is contained within the specification, and that while the precise terms appearing in the claims need not necessarily appear in the specification, there must be sufficient detail in the specification that a POSITA can clearly conclude that the invention described in the claims had been invented as of the filing date sought.

14. I have been informed that to satisfy the written description requirement, the specification must actually or inherently disclose each element of the claims.

15. I have been informed that for the disclosure to be inherent, the missing descriptive matter must necessarily be present in or unavoidably be taught by the specification, such that a POSITA would recognize such disclosure.

16. I have been informed that subject matter that is not disclosed, but would be obvious over what is expressly disclosed, does not satisfy the written description requirement.

17. I have been further informed that a claim is not patentable if the claimed invention was otherwise available to the public before the effective filing date of the claimed invention.

VIII. OVERVIEW OF THE SUBSTITUTE CLAIMS

A. TABLE CORRELATING ORIGINAL CLAIM TO SUBSTITUTE CLAIM

18. I understand that in Patent Owner's Motion to Amend, Patent Owner has sought to amend the independent claims by proposing new substitute claims. The table below compares the Original Claims to the Substitute Claims, with independent claims emphasized in bold italics.

Original Claim	Dependency	Substitute Claim	Dependency
<i>21</i>	None	<i>22</i>	None

B. LIST OF SUBSTITUTE CLAIM

19. Patent Owner also provided annotations showing the changes it made to the Original Claim 21 of the '959 Patent. This is found in "Claims Appendix" of the Motion to Amend. These changes are shown below.

20. Substitute Claim 22:

[22.pre] A device configured to communicate identification information associated with a low-altitude aircraft, the device comprising:

[22.a] a radio frequency communication antenna; and

[22.b] a radio communication module coupled to the radio frequency communication antenna and configured to transmit identification information associated with the low-altitude aircraft through a transmitted radio signal,

[22.c] wherein the radio communication module is configured to receive a [[received]] radio signal and store the received information in a storage,

[22.d] wherein the radio frequency communication antenna is coupled to the low-altitude aircraft and

[22.e] the radio communication module is configured to utilize a secure identifier, and

[22.f] the radio communication module is configured for two-way communication with a remote portable detection system; and

[22.g] wherein the device is coupled to the low-altitude aircraft and

[22.h] the remote portable detection system includes a user interface configured to provide to a user, information associated with a plurality of different low-altitude aircrafts detected by the remote portable detection system [[.]], and

[22.i] wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system for cross-verifying the secure identifier and the transmitted identification information, to verify authenticity of the transmitted identification information.

IX. PRIORITY DATE OF THE SUBSTITUTE CLAIM

21. In its Motion to Amend, PO asserts that the priority date of Substitute Claim 22 is June 12, 2015. MTA at 2-10 (purporting that the earliest written description support for the Substitute Claim is Exhibit 2016, which is U.S. Provisional Application No. 62/175,153). I disagree. For the same reasons discussed in the Petition and my original declaration, the Substitute Claim is not adequately supported by the '153 Prov. (EX2016), and Substitute Claim 22 is not entitled to claim priority to the '071 Application. Pet. at 7-16; EX1003, ¶¶70-78. At best, the '959 Patent's priority date is October 1, 2017, which is the filing date of U.S. Provisional Application No. 62/566,450.³ *Id.*

X. CLAIM CONSTRUCTION

³ I do not concede that U.S. Provisional Application No. 62/566,450 provides written description support for the Substitute Claim. Moreover, as I discuss below, the Substitute Claim is not even supported by the '959 Patent's underlying application which was filed on December 10, 2018.

22. I understand that “claim construction” is the process of determining a patent claim’s meaning. I also understand that, during an *inter partes* review, a claim construction analysis begins with the plain meaning of the claim term, which is the ordinary and customary meaning given to the term by those of ordinary skill in the art at the time of the invention. I also understand that the claims of a patent must be interpreted in light of the specification—that is, the claim language itself, the written description, and the figures in the patent—as well as the patent’s prosecution history and/or any reexamination history.

23. As I noted in my original declaration, a POSITA would understand all the claim terms to have their plain and ordinary meaning. EX1003, ¶80. I applied the plain and ordinary meaning, in the context of the ’959 Patent, for all claim terms in my original declaration, and I apply the plain meaning to the substitute claim terms as well. Additionally, I understand that the Board construed “secure identifier” as “a credential that can be used to securely verify the identity of a device, such as an airborne object or ground-based transmitter” in the Institution Decision (Paper 13). Paper 13 at 10. I have also applied this construction to my analysis as well.

XI. SUMMARY OF CONCLUSIONS AND GROUNDS FOR CHALLENGE

24. Based upon my review of the Petition, the Motion to Amend, the materials cited in my Original Declaration and this Second Declaration, and the materials listed in the LIST OF EXHIBITS above, it is my opinion that Substitute

Claim 22 of the '959 Patent is rendered obvious by the Grounds listed in the table below:

Ground	Substitute Claim	Basis (35 U.S.C. §)	Prior Art
5	22	103	Beard and Viggiano
6	22	103	Taveira, Wang, Gong, and Viggiano
7	22	103	Taveira, Qi, Gong, and Viggiano
8	22	103	Gong, Wang-II, and Viggiano
9	22	103	Beard and Byers
10	22	103	Taveira, Wang, Gong, and Byers
11	22	103	Taveira, Qi, Gong, and Byers
12	22	103	Gong, Wang-II, and Byers

25. It is further my opinion that Substitute Claim 22 is invalid as indefinite because a POSITA lacks reasonable certainty as to the scope of “to receive a radio signal” and “the received information” as recited in this claim.

26. It is additionally my opinion that Substitute Claim 22 is invalid for lack of written description because the specification of the '959 Patent does not reasonably convey to a POSITA that the inventor had possession of a “radio communication module” that transmits both “identification information” and a “secure identifier.”

27. Moreover, it is additionally my opinion that Substitute Claim 22 is invalid for lack of written description because the specification of the '959 Patent does not reasonably convey to a POSITA that the inventor had possession of a “the radio communication module is configured to utilize a secure identifier.”

XII. THE SUBSTITUTE CLAIM ENLARGES CLAIM SCOPE

28. In the MTA, PO amended element [22.c] of the Substitute Claim to recite “wherein the radio communication module is configured to receive a [[received]] radio signal.” MTA at 4. In my opinion, this amendment broadens the Substitute Claim because the claim now contemplates receiving any sort of “radio signal” (“receive *a* radio signal”). *Id.* I understand that PO state that this amendment addresses “a typographical correction.” MTA at 2. I do not agree, and I do not observe an apparent typographical error in element [22.c] that this amendment addresses. Hence, in my opinion, the amendment of element [22.c] enlarges the scope Substitute Claim 22.

XIII. THE SUBSTITUTE CLAIM LACKS WRITTEN DESCRIPTION SUPPORT

A. SUBSTITUTE CLAIM 22: ELEMENT [22.i]

29. Element [22.i] recites “wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system for cross-verifying the secure identifier and the transmitted identification information, to verify authenticity of the transmitted identification information.”

MTA at 8-9. Via this element, PO is attempting to claim a “radio communication module” that transmits both “identification information” and a “secure identifier.” MTA at 4-9 (elements [22.b] (“radio communication module...configured to transmit identification information...”), [22.e] (“the radio communication module is configured to utilize a secure identifier”), [22.i] (“utilizing the secure identifier comprises transmitting the secure identifier...”). In my opinion, this concept, as well as use of a “secure identifier” itself (i.e., in “cross-verifying” as recited by [22.i]), is not supported by the ’959 Patent.

30. PO cites to its analysis for element [22.e] as alleged support. PO states that “security identifier comprises a code that is ‘similar’ to the code that is ‘transmitted’ identification information, and the RF module transmits the similar code, i.e., the security identifier.” MTA at 8. As an initial matter, PO is referring to a claim element that is not recited by the claims (“*security* identifier”) which renders PO’s analysis inaccurate and wrong. Moreover, PO’s allegations are incorrect. As I discuss further below in Section XIII.B, the element [22.e] citations fail to disclose a “secure identifier” as claimed. Moreover, PO’s assertion that the element [22.e] citations describe an “RF module transmits the similar code, i.e., the security identifier” is wrong because they do not describe this. At best, EX2015 at 2:27-3:5 and 3:14-16 (and corresponding EX1001 at 2:30-59) describe an aircraft light array that blinks a color pattern, and a transponder that transmits a code via RF that is

“similar” to that blinked by the light array—not “similar” to some other code transmitted via a radio frequency (RF). In my opinion, none of this describes a radio communication module transmitting a “secure identifier” or the “cross-verifying” of such a “secure identifier” and “transmitted identification information.” I further note that the claim does not even say what performs “cross-verifying.”

31. PO also refers to the citations of element [22.pre]. MTA at 3, 8 These portions again relate to transmitting an “identification code” via a “visible light color sequence or by a radio frequency signal.” EX2015 at 2:11-17; EX1001 at 2:7-15; EX2016 at ¶29. None concern a “secure identifier,” let alone a radio communication module transmitting a “secure identifier,” or cross-verification involving a “secure identifier” as claimed.

32. The additional portions cited by PO also do not provide written description support. MTA at 8-10. They refer to either (1) a “ground identification device 21” that “can detect aircrafts through the RF signal transmitted from the identification box RF module 16” or (2) “command execution” and the communication of “execution results” including an “ACK” or “error status code” to “ground identification unit 21.” *See, e.g.*, EX1001 at 6:31-35, 7:54-8:6, Figs. 7, 8. PO has not shown or explained how they support a “secure identifier,” a radio communication module transmitting a “secure identifier,” or cross-verification that uses a “secure identifier.”

33. PO also cites to “EX1001 at 38-44,” but this citation is incomplete. MTA at 9. PO may be referring to the equivalent portion of EX2015 at 4:15-19, which is EX1001 at 3:38-44. However, this section also does not provide adequate written description support. The section states that a “remote (e.g., ground) device” is “equipped with a camera, lens, and image processing algorithms to capture the color sequence,” and that “[i]n addition, the device has an RF receiver capable of receiving the identification box RF signal to connect both information sources and to verify authenticity,” but this says nothing about a “secure identifier,” a radio communication module transmitting a “secure identifier,” or cross-verification that uses a “secure identifier.” EX1001 at 3:38-44.

34. Finally, PO provides commentary at the end of the element [22.i] analysis that purports to summarize PO’s cited sections. MTA at 9-10. This commentary is unclear, wrong, and disconnected from the sections because it refers to concepts that are not disclosed. PO states that “the ’406 App. and the ’153 Prov. each discloses that the ground device crosschecks / cross-verifies the ‘code,’ i.e., the transmitted identification information and a code similar to the code, i.e., the secure identifier, to verify authenticity of the transmitted identification information.” *Id.* at 9. However, for the same reasons discussed above, the citations do not show the verification of any “code” and “code similar to the code” that is a “secure identifier,” as PO confusingly purports.

35. PO also alleges that “[w]hen the light array transmits the command execution results, the light array does not transmit the code, i.e., the identification information” and “[i]n that event, the RF module of the identification box transmits to the ground device, using RF, the ‘same code,’ i.e., the identification information and a ‘similar code,’ i.e., the secure identifier.” MTA at 9-10. Yet again, PO’s comments are disconnected from the ’959 Patent’s disclosure and they find no support. PO has not shown any portion of the ’959 Patent that discloses an RF module that transmits both identification information and a secure identifier, including within the context of “command execution results.” Finally, PO’s allegation that such a transmitted identification information and secure identifier are verified (MTA at 10) is wrong and unsupported for the same reasons. In my opinion, PO has failed to demonstrate that element [22.i] has sufficient written description support.

36. At bottom, the ’959 Patent does not describe the cross-verifying functionality using a “secure identifier” and “identification information.” A POSITA would not have understood that the specification demonstrates possession of the subject matter recited in the Substitute Claim.

B. SUBSTITUTE CLAIM 22: ELEMENT [22.E]

37. Element [22.e] recites “the radio communication module is configured to utilize a secure identifier.” MTA at 5. In my opinion, PO has not demonstrated written description support for this element.

38. As background information for element [22.e], Substitute Claim 22 recites a “device” that comprises “the radio communication module” of element [22.e]. MTA at 3-6 (elements [22.pre], [22.b], [22.e]). The claim requires that “the device is coupled to the low-altitude aircraft.” *Id.* at 7 (element [22.g]). Thus, the “radio communication module” is coupled to the low-altitude aircraft, and therefore on-board the aircraft. I note that PO agrees with this contention, alleging that the written description’s “RF module” corresponds to the claimed “radio communication module” and stating that the RF module is “included in the identification box that is attached to the low-altitude aircraft.” MTA at 4-5 (elements [22.b], [22.c], [22.d]).

39. However, I note that PO’s alleged written description support for element [22.e] does not reference disclosure concerning a “radio communication module” that is on-board an aircraft and utilizes a “secure identifier.” MTA at 5-6. PO first cites to EX2015 at 4:14-20 and 4:25-26, as well as EX2016 at ¶¶11-12 and EX1001 at 3:37-44 and 3:53-55. MTA at 5. These sections refer only to a “ground” based device rather than a component that is on-board an aircraft. In particular,

EX1001 at 3:37-44 and 3:53-55 and EX2015 at 4:14-20 and 4:25-26 are located under a heading titled “Ground Identification Device” and describe a “remote (e.g., ground)” device that “assist[s] the aircraft identification.” EX1001 at 3:37-44 (also describing “the ground device”), 3:53-55; EX2015 at 4:14-20, 4:25-26. EX2016 at ¶¶11-12 centers on how “a ground device to assist the aircraft identification has been invented.” These sections therefore cannot provide written description support for the claimed “radio communication module” that is on-board an aircraft and that “is configured to utilize a secure identifier.”

40. PO also cites to EX2015 at 3:4-5 and 3:14-16, EX2016 at ¶¶7 and 8, and EX1001 at 2:41-42 and 2:56-59. These sections also fail to provide written description support for element [22.e]. These sections describe use of a “transponder” that transmits a code via an RF frequency, where the code corresponds to a sequence of blinked lights generated by an aircraft light array. *See, e.g.* EX2015 at 2:27-3:5, 3:14-16; EX1001 at 2:30-59. PO has not shown that these sections describe using a “secure identifier” (or otherwise explain what a “secure identifier” is), let alone a “radio communication module” that is on board an aircraft and configured to “utilize a secure identifier.”

41. I finally note that PO provides commentary at the end of the element [22.e] analysis that purports to summarize PO’s cited sections. This commentary is wrong. PO states that “the ’406 App. and the ’153 Prov. both teach that the ground

station crosschecks / cross-verifies two identifiers – the ‘code,’ i.e., the transmitted identification information, which can be transmitted through RF, and another ‘similar’ code, i.e., the security identifier.” MTA at 6. PO again refers to a “security identifier” that is not recited in Substitute Claim 22, and PO’s commentary is thus irrelevant. Additionally, contrary to the commentary, PO has not shown that the cited sections describe use of a “secure identifier” as claimed (or a “security identifier”), let alone cross checking or cross verifying that uses a “secure identifier,” rendering PO’s comments baseless.

42. I also note the following issue with respect to element [22.e]. For the same reasons discussed in the Petition and my original declaration, element [22.e] is not adequately supported by the ’153 Prov. (EX2016), and Substitute Claim 22 is not entitled to claim priority to PCT/US2016/037071 (“the ’071 Application”). Petition, 7-16; EX1003, ¶¶70-78. I note that the Board recognized this in the Institution Decision (Paper 13), 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 Substitute Claim 22. Paper 13 at 11-14. In my opinion, the MTA does not properly address the Board’s analysis of the Institution Decision or otherwise address the priority issues raised by the Petition. The MTA generically states that “[i]n proposed substitute claim 22, ‘utilize secure identifier’ is defined in a manner that is consistent with the Board’s interpretation

and that is fully supported by both the '406 App. and the '153 provisional” and refers to Section IV of the MTA. MTA at 11. But none of this changes the Board’s correct determination of the Institution Decision. Decision, Paper 13 at 11-14. Substitute Claim 22 recites the same “secure identifier” as claim 21 and newly added limitation [22.i] simply attempts to explain how the “secure identifier” is “utilize[d]”—not what the term “secure identifier” itself means. MTA at 8-9 (element [22.i]).

43. Thus, in my opinion, Substitute Claim 22 still suffers from the very same written description issues determined by the Board with respect to original claim 21. Moreover, PO’s reference to Section IV of the MTA noted above is without merit because, as discussed above, the MTA’s cited portions for element [22.e] (which are contained in Section IV of the MTA) do not provide adequate written description support. In my opinion, PO has thus failed to demonstrate that element [22.e] has sufficient written description support.

XIV. THE SUBSTITUTE CLAIM IS INDEFINITE

A. SUBSTITUTE CLAIM 22: ELEMENT [22.C]

44. Element [22.c] recites “wherein the radio communication module is configured to receive a [[received]] radio signal and store the received information in a storage.” MTA at 4. In my opinion, this element renders Substitute Claim 22 indefinite for multiple reasons.

45. First, Substitute Claim 22 previously recites in element [22.b] “a transmitted radio signal.” MTA at 4. In my opinion, it is thus unclear in element [22.c] whether “to receive a radio signal” refers to receiving the same transmitted radio signal of element [22.b], or to receive some other radio signal. For this reason alone, in my opinion, the scope of Substitute Claim 22 is ambiguous and unclear, rendering the claim indefinite.

46. Second, the term “the received information” of element [22.c] lacks antecedent basis because it could refer to multiple previously recited terms within Substitute Claim 22. This also makes the claim indefinite. The claim previously recites to “transmit identification information associated with the low-altitude aircraft through a transmitted radio signal” in element [22.b]. MTA at 4. Thus, in my opinion, “the received information” in element [22.c] could refer to the “identification information” that is transmitted in element [22.b] due to the common usage of “information” in both terms. However, Substitute Claim 22 also recites “to receive a radio signal” in element [22.c]. *Id.* Thus, in my opinion, “the received information” could also refer to the received “radio signal” due to the common usage of “receive” and “received” in both terms. Thus, “the received information” of element [22.c] lacks adequate antecedent basis and, in my opinion, a POSITA would not have been able to ascertain the scope of PO’s alleged invention, which renders the claim indefinite.

XV. THE SUBSTITUTE CLAIM IS OBVIOUS

47. In my opinion, the Substitute Claim would have been obvious under 35 U.S.C. §103 in view of the following grounds. In the grounds, I address the limitations from the Substitute Claim added by PO in the MTA and certain other relevant limitations; limitations from the original claim not addressed below are addressed in the Petition and in my original declaration. I note that elements that are indefinite and/or lack written description support are addressed based on my understanding of PO's position and as best understood by a POSITA.

48. In particular, Grounds 5-8 rely on the original grounds from the Petition and add Viggiano (EX1024). Grounds 9-12 rely on the original grounds from the Petition and add Byers (EX1025).

49. Viggiano (EX1024) (published October 11, 2007; filed April 7, 2006) is prior art to the Substitute Claim under 35 U.S.C. §102(a)(1) and (a)(2) even if the claim is entitled to the '959 Patent's earliest claimed priority date of June 12, 2015 (which it is not). *See* Section IX.

50. Byers (EX1025) (filed March 28, 2016) is prior art to the Substitute Claims under 35 U.S.C. §102(a)(2) as the '959 Patent is entitled to a priority date no earlier than October 1, 2017. *See* Section IX.

51. In my opinion, because Viggiano and Byers each address aircraft identification techniques, they are each highly relevant to the '959 Patent. EX1001,

1:28-31, 2:27-29; EX1024, Abstract, ¶¶0002, 0012-0018, 0024-0027, Figs. 1, 3; EX1025, Abstract, 8:21-35, 8:65-9:24, 9:48-10:5, 10:30-11:26, Figs. 3, 4.

A. OVERVIEW OF VIGGIANO (EX. 1024)

52. Viggiano discloses a “system for authenticating the identity of ADS-B systems.” EX1024, Abstract. Viggiano’s system involves generating a “message authentication code” (MAC) 38 from an ADS-B transmitter (and thus aircraft) identification information 22 and secret key 36 which is “unique” to the transmitter (and thus aircraft). *Id.*; EX1024, ¶¶0012-0015, 0019-0027, Figs. 1-3. Moreover, information 22 may be encrypted when it is used to form MAC 38, and MAC 38 is generated by using a “secure hash algorithm” and a “moving bit pattern” that truncates the result of the algorithm. *Id.*, ¶¶0017, 0019, 0026-0027. The MAC 38 is transmitted to an authenticator 10 by the ADS-B transmitter. *Id.*, ¶¶0002, 0012-0019, 0024-0027, 0028, Figs. 1-3.

53. Viggiano further discloses that identification information 32 is also transmitted by the ADS-B transmitter to authenticator 10. EX1024, ¶¶0002, 0012-0019, 0024-0027, 0028, Figs. 1-3, Claims 1, 5, 8, 21, 39. The authenticator 10 generates a MAC 58 using identification information 32. *Id.* The MAC 38 and MAC 58 are then compared by comparator 70 to determine a match. *Id.* If a match exists, the identity of the ADS-B transmitter (and thus aircraft) is authenticated. *Id.*

54. I note that Viggiano discloses embodiments in which a “challenge-response methodology” between the ADS-B transmitter and the Authenticator is employed. EX1024, ¶0012. However, I also note that Viggiano’s system is not so limited to “challenge-response,” and Figure 2 shows an example technique of “identity authentication” using the same components described in relation to Figure 1 and Figure 3 but “without using the authentication challenge-response methodology for airspace.” *Id.*, ¶0019, Fig. 2.

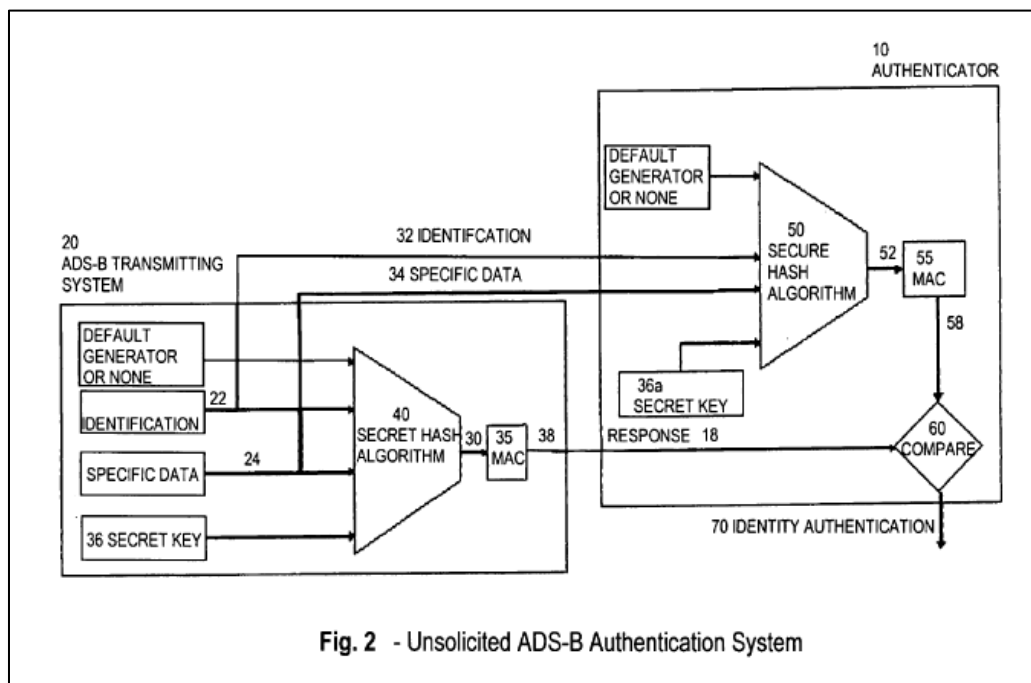


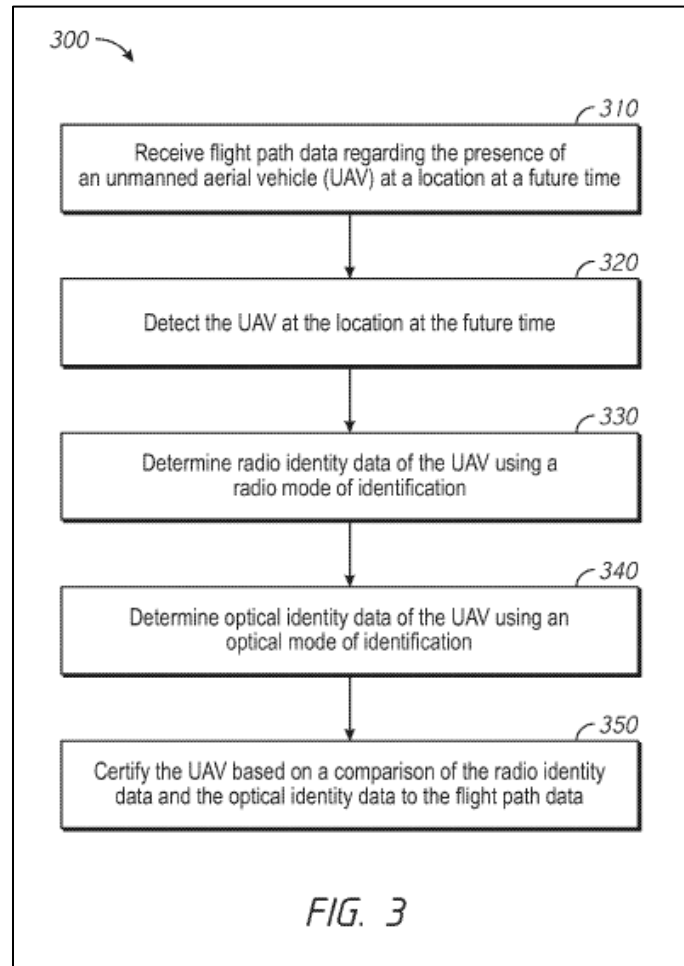
Fig. 2 - Unsolicited ADS-B Authentication System

EX1024, Fig. 2

B. OVERVIEW OF BYERS (EX. 1025)

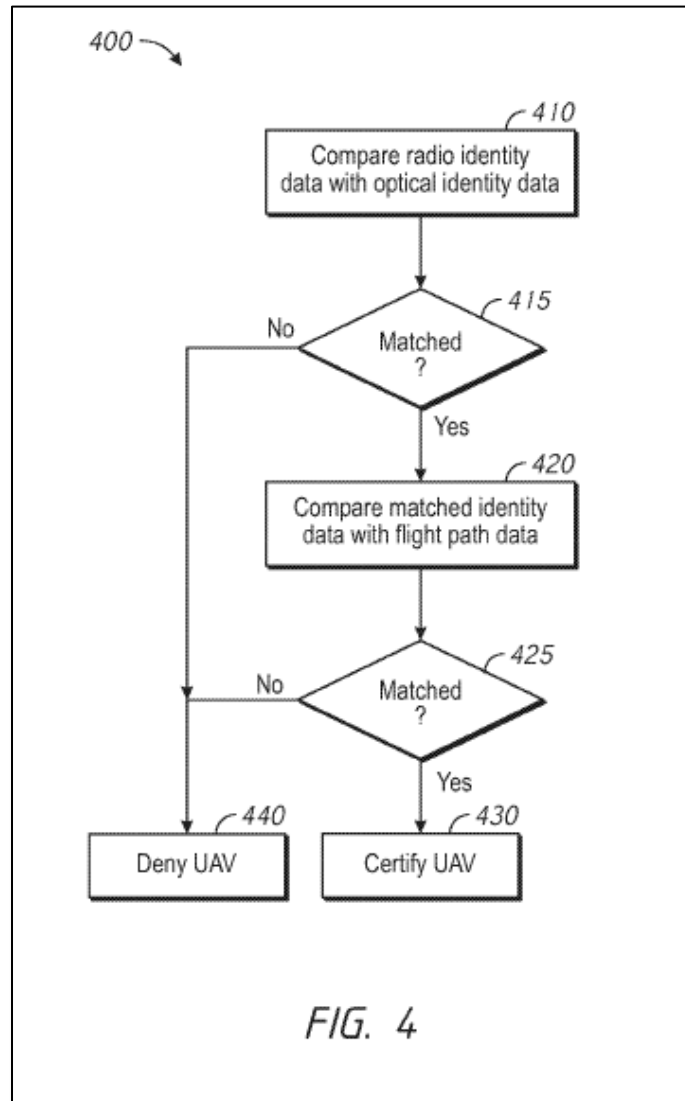
55. Byers discloses unmanned aerial vehicle (UAV) authentication using “multiple modes of identification.” EX1025, 10:40-61, Fig. 4. One mode is a “radio mode” in which encrypted telemetry packets that include a UAV identifier are

transmitted by the UAV via RF to a receiving device. *Id.*, 5:35-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, Fig. 3. Another mode is “another radio mode of identification” where “additional radio identity data” of the UAV is transmitted by the UAV to the receiver. *Id.*, 9:66-10:5, 10:30-39, Fig. 3. A further mode is an “optical mode of identification” in which “optical identity data of the UAV” is transmitted by the UAV to the receiver via a modulated light stream representing the UAV identity. *Id.*, 5:9-35, 9:25-47, Fig. 3. With respect to Figure 3, Byers discloses an embodiment in which all three of these identification modes are used by a receiving device to “certify” a UAV. *Id.*, 4:38-44, 6:61-7:8, 10:30-39, Fig. 3.



EX1025 (Byers), Fig. 3

56. With respect to Figure 4, Byers discloses another embodiment in which “radio identity data (determined by a radio mode of identification)” is compared with “optical identity data (determined by an optical mode of identification)” by the receiving device, where if a match results from the comparison the UAV is “authenticated.” *Id.*, 4:38-44, 6:61-7:8, 10:53-61, Fig. 4. This is in step 410. *Id.*



EX1025 (Byers), Fig. 4

C. GROUND 5: BEARD AND VIGGIANO

1. Motivation to Combine

57. A POSITA would have been motivated to combine Beard and Viggiano with a reasonable expectation of success. As combined, the Beard-Viggiano system would have provided the predictable result in which Beard's unmanned aerial system (UAS) RF transceiver utilizes Viggiano's teachings of transmitting a "message authentication code" (MAC) 38 formed by encrypted identification information 22 and secret key of the UAS and transmitting identification information 32 of the UAS, and that Beard's receiver verifies the identity of the UAS by determining a MAC 58 from information 32 and comparing the two MACs 38 and 58 to determine a match and "authenticate" aircraft identity. EX1008, Abstract, 3:30-36, 4:61-5:7, 5:41-57, 8:39-42, 9:8-12, 10:12-20; EX1009, 3-8, 11; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39. A POSITA would have been so motivated because the use of false or fraudulent identity information by a UAV was known problem in the art. EX1024, ¶¶0003-0007; Viggiano addresses this problem and furthers Beard's own verification teachings, providing a specific technique for aircraft identity verification that aims to prevent "unauthorized third parties" from "enter[ing] a given air traffic control region by broadcasting false identification data." EX1024, ¶0004. Indeed, Beard already discloses the general verification of UAS identity using transmitted identification information, and a POSITA would have recognized that Viggiano provides implementation details for performing such verification, 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. And both Beard and Viggiano teach determining accurate aircraft identity and both utilize ADS-B for aircraft data transmissions, further demonstrating the compatibility of the references and complementary nature of their teachings. 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. As such, a POSITA would have had a reasonable expectation of success in making the combination.

2. Element [22.b]

58. Beard's remote identification (RID) device attached to an unmanned aircraft system (UAS) includes an RF transceiver (*radio communication module*). Pet. at 29-31. The Beard-Viggiano combination teaches that the RF transceiver transmits identification information 32, which can be encrypted and identifies Beard's UAS aircraft (*configured to transmit identification information associated with the low-altitude aircraft*). *Id.*; 0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section XV.C.1. The remaining aspects of element [22.b] are as in the Petition. Pet., 29-31.

3. Element [22.c]

59. 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.*”

60. The Beard-Viggiano combination teaches to “*store the received information in a storage.*” If “*the received information*” is interpreted to refer to the “*identification information associated with the low-altitude aircraft*” recited in element [22.b], Beard-Viggiano combination discloses that Beard’s RID device can “store[] to memory” the “current position of the UAS 102 and identification data” of the UAS associated with the RID device, which would have thus included Viggiano’s identification information in the combination. EX1008, 5:44-46, 7:45-47; EX1009, 11, 15; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section III.B.1.a EX1003, ¶125; Pet. at 31-34. If “*the received information*” is interpreted to refer to information associated with the “radio signal” recited in element [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.***” EX1008, 7:45-48 (emphasis added), 7:48-51; EX1009, 15; EX1003, ¶126; Pet., 31-34.

4. Elements [22.e] and [22.i]

61. Beard's RF transceiver forms a "*radio communication module*." Section XV.C.2. Beard's receiver forms a "*remote portable detection system*." Pet., 35-39. The Beard-Viggiano combination teaches that Beard's RF transceiver transmits a message authentication code (MAC) 38 to Beard's receiver (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system*). EX1008, 3:30-36, 5:41-57, 7:11-17, 8:39-42, 9:8-12, 9:67-10:20; EX1009, 3-8, 11, 15; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section III.B.1.a; Pet., 34-35. MAC 38 is a *secure identifier* for several reasons. First, MAC 38 is formed by identification information 22 that identifies the transmitting aircraft, as well as secret key 36 which is "unique" to the aircraft, which makes MAC 38 an *identifier* of the transmitting aircraft. *Id.*; EX1024, ¶¶0012-0015, 0019-0027, Figs. 1-3. Moreover, information 22 may be encrypted when it is used to form MAC 38, and MAC 38 is generated by using a "secure hash algorithm" and a "moving bit pattern" that truncates the result of the algorithm. *Id.*, ¶¶0017, 0019, 0026-0027. MAC 38 is also generated from use of a "secret key" which further aids in security by assuring that the transmitted MAC is "from the aircraft that the message claims it to be from." *Id.*, ¶0022. All of these aspects make MAC 38 *secure*.

62. The combination teaches that the MAC 38 (*secure identifier*) is received by the receiver, which then compares the MAC 38 to another MAC 58 that is formed from the separately transmitted identification signal 32, to “authenticate” transmitter identity. Pet., 34-35; EX1024, ¶¶0002, 0012-0019, 0024-0027, 0028, Figs. 1-3, Claims 1, 5, 8, 21, 39. By comparing MAC 58 and 38 to authenticate identity, a POSITA would have understood that the identification information 32 and identification information 22 that respectively form each MAC would have been cross verified with each other, and that this process would have authenticated the identity of the transmitter UAV and thus authenticated the transmitted identification information 32 representing this identity (*“for cross-verifying the secure identifier and the transmitted identification information, to verify authenticity of the transmitted identification information”*). *Id.* I also note that because MAC 38 (*secure identifier*) is used in this authentication process described above to authenticate identity of the transmitter UAV, and because MAC 38 is generated from (1) encrypted information 22, (2) using a “secure hash algorithm” and a “moving bit pattern,” and (3) use of a “secret key,” it teaches the Board’s construction of *secure identifier* as “a credential that can be used to securely verify the identity of a device, such as an airborne object or ground-based transmitter” as noted in the Institution Decision (Paper 13). EX1024, ¶¶0017, 0019, 0022, 0026-0027; Paper 13 at 10.

Moreover, the Petition also taught the Board's construction of *secure identifier* as well. Pet. at 34-35.

D. GROUND 6 AND 7: TAVEIRA, WANG, GONG, AND VIGGIANO (GROUND 6)/TAVEIRA, QI, GONG, AND VIGGIANO (GROUND 7)

1. Motivation to Combine

63. A POSITA would have been motivated to combine Taveira, Wang, and Gong/Taveira, Qi, and Gong as discussed in the Petition, and would have further been motivated to combine each combination with Viggiano with a reasonable expectation of success. Pet. at 40-45, 60-62; EX1003, ¶¶138-146, 172-176. Viggiano provides advantageous techniques for aircraft identity verification that mitigates against fraudulent/false UAV identifiers, as I note above. Section XV.C.1. In my opinion, a POSITA thus would have been motivated to make the combinations of Taveira, Wang, Gong, and Viggiano, as well as Taveira, Qi, Gong, and Viggiano, to achieve these advantages. *Id.* The combinations would have each provided the predictable result in which Taveira's drone radio module 130 transmits a MAC 38 formed by encrypted identification information 22 and a secret key, and transmits identification information 32, and a receiving device verifies the identity of the drone by determining a MAC 58 from information 32 and comparing the two MACs 38 and 58 to determine a match and "authenticate" aircraft identity. *Id.*; Pet. at 40-45, 60-62; EX1003, ¶¶138-146, 172-176; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39.

2. **Element [22.b]**

64. Taveira's radio module 130 forms a *radio communication module*. Pet. at 49-50, 62. In the combinations, radio module 130 transmits identification information 32 that identifies Taveira's drone (*configured to transmit identification information associated with the low-altitude aircraft*). *Id.*; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section XV.D.1. The combinations each teaches the remaining aspects of element [22.b] for the same reasons discussed in the Petition. Pet., 49-50, 62.

3. **Element [22.c]**

65. 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. The combinations each teach to “*store the received information in a storage*.” If “*the received information*” is refers to the “*identification information associated with the low-altitude aircraft*” of [22.b], the combinations disclose storing identification data associated with the drone, which would have included access level information. Pet., 50-53, 62; Section XV.D.1. If “*the received information*” is 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. Pet., 50-53, 62.

4. **Elements [22.e] and [22.i]**

66. Radio module 130 forms a “*radio communication module*.” Section XV.D.2. Taveira and Gong teach a device that forms a “*remote portable detection system*.” Pet. at 55-58. The combinations each teach that radio module 130 transmits a MAC 38 to the device (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system*). Pet. at 53-55; Section XV.D.1; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39. MAC 38 is a *secure identifier* for at least the reasons discussed in Section XV.C.4 and further meets the Board’s construction for the reasons discussed in that Section. Moreover, the combinations each teach that the device forms a MAC 58 from identification information 32, and the MAC 58 and MAC 38 (*secure identifier*) are compared to each other by a comparator to “authenticate” the identity of the transmitter UAV. EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section XV.D.1. This comparison teaches *for cross-verifying the secure identifier and the transmitted identification information, to verify authenticity of the transmitted identification information* for the same reasons discussed in Section XV.C.4. Moreover, the Petition also taught the Board’s construction of *secure identifier* as well. Pet. at 53-55, 62-64.

E. GROUND 8: GONG, WANG-II, AND VIGGIANO

67. Elements [22.b], [22.e], and [22.i] are addressed below. The remaining claim elements, including element [22.c], are addressed as in the petition.

1. Motivation to Combine

68. A POSITA would have been motivated to combine Gong and Wang-II as discussed in the Petition and my original declaration, and would have further been motivated to combine with Viggiano with a reasonable expectation of success. Pet. at 64-66; EX1003, ¶¶188-191. Viggiano provides advantageous techniques for aircraft identity verification that mitigates against fraudulent/false UAV identifiers. Section XV.C.1. The Gong-Wang-II-Viggiano combination would have thus provided the predictable result in which Gong's communication module/unit of a drone transmits a MAC 38 formed by encrypted identification information 22 and a secret key of the drone, and transmits identification information 32 of the drone, and a geo-fencing device verifies the identity of the drone by determining a MAC 58 from information 32 and comparing the two MACs 38 and 58 to determine a match and "authenticate" aircraft identity. *Id.*; Pet. at 64-66; EX1003, ¶¶188-191; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39.

2. Element [22.b]

69. Gong's communication module/unit forms a *radio communication module*. Pet., 70-72. In the combination, the communication module/unit transmits identification information 32 that identifies Gong's drone (*configured to transmit*

identification information associated with the low-altitude aircraft). *Id.*; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section XV.E.1. Gong-Wang-II teaches the remaining aspects of [22.b] for the same reasons as in the Petition. Pet., 70-72.

3. **Element [22.e] and [22.i]**

70. Gong's communication module/unit forms a *radio communication module*. Pet. at 70-72. Gong's geofencing device that forms a “*remote portable detection system*.” Pet., 75-76. The combination teaches that Gong's communication module/unit transmits a MAC 38 to the geofencing device (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system*). Pet., 74-75; Section XV.E.1; EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39. MAC 38 is a *secure identifier* for at least the reasons discussed in Section XV.C.4 and further meets the Board's construction for the reasons discussed in that Section. Moreover, the combination teaches that the geofencing device forms a MAC 58 from identification information 32, and the MAC 58 and MAC 38 (*secure identifier*) are compared to each other by a comparator to “authenticate” the identity of the transmitter UAV. EX1024, ¶¶0002, 0011-0028, Figs. 1-3, Claims 1, 5, 8, 21, 39; Section XV.E.1. This comparison teaches *for cross-verifying the secure identifier and the transmitted identification information, to*

verify authenticity of the transmitted identification information for the same reasons discussed in Section XV.C.4. Moreover, the Petition also taught the Board’s construction of *secure identifier* as well. Pet. at 74-75.

F. GROUND 9: BEARD AND BYERS

1. Motivation to Combine

71. A POSITA would have been motivated to combine Beard and Byers with a reasonable expectation of success.

72. **Combination of Byers embodiments:** Byers discloses unmanned aerial vehicle (UAV) authentication using “multiple modes of identification.” EX1025, 10:40-61, Fig. 4. One mode is a “radio mode” in which encrypted telemetry packets that include a UAV identifier—encrypted radio identity data—are transmitted by the UAV via RF to a receiving device. *Id.*, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, Fig. 3. Another mode is “another radio mode of identification” where “additional radio identity data” of the UAV is transmitted by the UAV to the receiver. *Id.*, 9:66-10:5, 10:30-39, Fig. 3. A further mode is an “optical mode of identification” in which “optical identity data of the UAV” is transmitted by the UAV to the receiver via a modulated light stream representing the UAV identity. *Id.*, 5:9-35, 9:25-47, Fig. 3. With respect to Figure 3, Byers discloses an embodiment in which all three of these identification modes (i.e., using encrypted radio identity data, additional radio identity data, and optical identity data) are used by a receiving

device to “certify” a UAV. *Id.*, 4:38-44, 5:9-51, 5:58-6:46, 6:61-7:8, 10:30-39, Fig. 3. With respect to Figure 4, Byers discloses another embodiment in which “radio identity data (determined by a radio mode of identification)” is compared with “optical identity data (determined by an optical mode of identification)” by the receiving device, where if a match results from the comparison the UAV is “authenticated.” *Id.*, 4:38-44, 5:9-51, 5:58-6:46, 6:61-7:8, 10:53-61, Fig. 4. A POSITA would have been motivated to combine the Figure 3 and Figure 4 embodiments such that the encrypted “radio identity data” and “additional radio identity data” are compared to each other to determine a match to authenticate the UAV, with a reasonable expectation of success. *Id.*, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4. This combination would have been a predictable variation of Byers’ teachings that a POSITA would have readily implemented, and it would not have required a leap of inventiveness to combine the two embodiments. I note that the Figure 3 and Figure 4 descriptions and figures themselves are disclosed next to each other in Byers. And as discussed, Byers describes authenticating UAV identity using two of the disclosed identification modes—radio mode and optical mode—and it would have been predictable to simply use one of the other disclosed modes—the additional radio mode—instead of the optical mode in this authentication process. By providing yet another technique for UAV authentication, the combination of embodiments would have

furthered Byers' goal of "implement[ing] highly robust and trustworthy systems and method[s] to identify individual UAVs, e.g., using various modes of generating identification information." EX1025, 3:25-28. Moreover, a POSITA would have been motivated to perform this combination due to the known limitations of using an "optical mode" (e.g., modulated light stream, such as blinking lights) such as the requirement of maintaining line of sight between the transmitter of the lights and a receiver. Indeed, occlusion of the light stream due to buildings, trees, and weather artifacts, for example, would have presented potential problems in deciphering identity from the light stream. As such, a POSITA would have been further motivated for this additional reason to utilize the encrypted "radio identity data" and "additional radio identity data," instead of the optical data. And in view of the above, for the reasons discussed, the combination would have had a reasonable expectation of success and would have been routine for POSITAs to perform.

73. **Combination of Beard and Byers:** A POSITA would have been motivated to combine Beard and Byers. The Beard-Byers combination would have provided the predictable result in which Beard's UAS RF transceiver transmits encrypted radio identity data and additional radio identity data to Beard's receiver, which compares the data to determine a match and authenticate the UAV, with a reasonable expectation of success. EX1008, Abstract, 3:30-36, 4:61-5:7, 5:41-57, 8:39-42, 9:8-12, 10:12-20; EX1009, 3-8, 11; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2,

8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4. A POSITA would have been so motivated because the use of false or fraudulent identity information by a UAV, including the “spoofing” of UAV identity, was a known problem in the art. EX1024, ¶¶0003-0007; EX1025, 1:15-17, 2:57-64, 3:35-37, 4:41-44, 5:6-8. Byers addresses this problem and furthers Beard’s own verification teachings, providing a specific technique for aircraft identity authentication that “increase[s] the difficulty of spoofing” and identity misrepresentation. EX1025, 3:35-37, 4:38-44. Indeed, Beard already discloses the general authentication UAS identity using transmitted identification information, and a POSITA would have recognized that Byers implementation details for performing such authentication, 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; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4. As such, a POSITA would have had a reasonable expectation of success in making the combination.

2. Element [22.b]

74. Beard’s RF transceiver discloses a *radio communication module*. Section XV.C.2. The Beard-Byers combination teaches that the RF transceiver transmits encrypted radio identity data of Beard’s UAS (*configured to transmit identification information associated with the low-altitude aircraft*). *Id.*; Pet., 29-31; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61,

Figs. 3, 4; Section XV.F.1. Beard teaches the remaining aspects of element [22.b] for the same reasons discussed in the Petition. Pet., 29-31.

3. Element [22.c]

75. Beard teaches “*wherein the radio communication module is configured to receive a radio signal.*” Section XV.C.3. The Beard-Byers combination further teaches to “*store the received information in a storage.*” If “*the received information*” refers to the “*identification information associated with the low-altitude aircraft*” recited in element [22.b], Beard-Byers combination discloses that Beard’s RID device attached to the UAS can “store[] to memory” the “current position of the UAS 102 and identification data” of the UAS associated with the RID device, which would have thus included Byers’ radio identity data in the combination. EX1008, 5:44-46, 7:45-47; EX1009, 11, 15; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.F.1; EX1003, ¶125; Pet. at 31-34. If “*the received information*” is interpreted to refer to information associated with the “radio signal” recited in element [22.c], Beard discloses that “the 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.***” EX1008, 7:45-48 (emphasis added), 7:48-51; EX1009, 15; EX1003, ¶126; Pet. at 31-34.

4. Elements [22.e] and [22.i]

76. Beard's RF transceiver forms a "*radio communication module*." Section XV.F.3. Beard's receiver forms a "*remote portable detection system*." Pet. at 35-39. The Beard-Byers combination teaches that Beard's RF transceiver transmits an encrypted radio identity data and additional radio identity data to Beard's receiver (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system*). EX1008, 3:30-36, 5:41-57, 7:11-17, 8:39-42, 9:8-12, 9:67-10:20; EX1009, 3-8, 11, 15; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.F.1; Pet., 34-35. The receiver compares the encrypted radio identity data and the additional radio identity data (*for cross-verifying the secure identifier and the transmitted identification information*) to determine a match and authenticate the UAV (*to verify authenticity of the transmitted identification information*). EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.F.1. I also note that the encrypted radio identity data (*secure identifier*) is used in this authentication process described above to authenticate the UAV, and because the radio identity data is encrypted, it teaches the Board's construction of *secure identifier* as "a credential that can be used to securely verify the identity of a device, such as an airborne object or ground-based transmitter" as noted in the Institution Decision (Paper 13). *Id.*; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5,

10:30-39, 10:53-61, Figs. 3, 4; Paper 13 at 10. Moreover, the Petition also taught the Board's construction of *secure identifier* as well. Pet. at 34-35.

G. GROUND 10 AND 11: TAVEIRA, WANG, GONG, AND BYERS (GROUND 10)/TAVEIRA, QI, GONG, AND BYERS (GROUND 11)

1. Motivation to Combine

77. A POSITA would have been motivated to combine Taveira, Wang, and Gong/Taveira, Qi, and Gong as in the Petition, and would have further been motivated to combine each of these combinations with Byers with a reasonable expectation of success. Pet. at 40-45, 60-62; EX1003, ¶¶138-146, 172-176. Byers provides advantageous techniques for UAV authentication that mitigates against spoofing and the use of false UAV identities. Section XV.F.1. A POSITA would have thus been motivated to make the combinations to achieve these advantages. *Id.* The combinations would have provided the predictable result in which Taveira's radio module 130 of a drone transmits encrypted radio identity data and additional radio identity data to a receiving device, which compares the data to determine a match and authenticate the UAV. *Id.*; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4.

2. Element [22.b]

78. Taveira's radio module 130 forms a *radio communication module*. Pet. at 49-50, 62. In the combinations, the radio module 130 transmits encrypted radio identity data of Taveira's drone (*configured to transmit identification information*

associated with the low-altitude aircraft). *Id.*; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.G.1. The combinations each teach the remaining aspects of element [22.b] for the same reasons discussed in the Petition. Pet. at 49-50, 62.

3. Element [22.c]

79. 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. The combinations teach to “*store the received information in a storage*.” 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, which would have included access level information. Pet., 50-53, 62; Section XV.G.1. 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. Pet., 50-53, 62.

4. Elements [22.e] and [22.i]

80. Radio module 130 forms a “*radio communication module*.” Section XV.G.2. Taveira and Gong teach a device that forms a “*remote portable detection system*.” Pet. at 55-58. The combinations teach that radio module 130 transmits encrypted radio identity data to the device (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier*

comprises transmitting the secure identifier to the remote portable detection system). Pet., 53-55; XV.G.1; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4. Moreover, the combinations teach that the receiving device compares the encrypted radio identity data and the additional radio identity data (*for cross-verifying the secure identifier and the transmitted identification information*) to determine a match and authenticate the UAV (*to verify authenticity of the transmitted identification information*). EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.G.1. The encrypted radio identity data is a *secure identifier* for the reasons discussed in Section XV.F.4. Moreover, the Petition also taught the Board's construction of *secure identifier* as well. Pet. at 53-55, 62-64.

H. GROUND 12: GONG, WANG-II, AND BYERS

1. Motivation to Combine

81. A POSITA would have been motivated to combine Gong and Wang-II as discussed in the Petition, and would have further been motivated to combine with Byers with a reasonable expectation of success. Pet. at 64-66; EX1003, ¶¶188-191. Byers provides advantageous techniques for UAV authentication that mitigates against spoofing and the use of false UAV identities. Section XV.F.1. A POSITA would have thus been motivated to make the combination to achieve these advantages. *Id.* The combination would have provided the predictable result in

which Gong's communication module/unit of a drone transmits encrypted radio identity data and additional radio identity data to a receiving device, which compares the data to determine a match and authenticate the UAV. *Id.*; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4.

2. Element [22.b]

82. Gong's communication module/unit forms a *radio communication module*. Pet. at 70-72. In the combination, the communication module/unit transmits encrypted radio identity data of Gong's drone (*configured to transmit identification information associated with the low-altitude aircraft*). *Id.*; EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.H.1. Gong-Wang-II teaches the remaining aspects of element [22.b] for the same reasons as in the Petition. Pet., 70-72.

3. Element [22.e] and [22.i]

83. Gong's communication module/unit forms a *radio communication module*. Pet., 70-72. Gong's geofencing device forms a "*remote portable detection system*." Pet., 75-76. The combination teaches that Gong's communication module/unit transmits encrypted radio identity data to the device (*the radio communication module is configured to utilize a secure identifier...wherein, utilizing the secure identifier comprises transmitting the secure identifier to the remote portable detection system*). Pet., 74-75; Section XV.H.1; EX1025, 5:9-51,

5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4. Moreover, the combination teaches that the receiving device compares the encrypted radio identity data and the additional radio identity data (*for cross-verifying the secure identifier and the transmitted identification information*) to determine a match and authenticate the UAV (*to verify authenticity of the transmitted identification information*). EX1025, 5:9-51, 5:58-6:46, 7:61-8:2, 8:65-9:24, 9:66-10:5, 10:30-39, 10:53-61, Figs. 3, 4; Section XV.H.1. The encrypted radio identity data is a *secure identifier* for the reasons discussed in Section XV.F.4. Moreover, the Petition also taught the Board's construction of *secure identifier* as well. Pet. at 74-75.

XVI. CONCLUSION

84. All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. I further understand that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code. I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 9, 2026.



Dr. Girish Chowdhary