

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

U.S. Patent No. 10,249,199

**SECOND DECLARATION OF NIKOLAOS PAPANIKOLOPOULOS, PH.D.
IN SUPPORT OF PATENT OWNER’S REPLY TO
PETITIONERS’ OPPOSITION TO
PATENT OWNER’S REVISED MOTION TO AMEND**

TABLE OF CONTENTS

I.	INTRODUCTION	8
II.	COMPENSATION	9
III.	MATERIALS CONSIDERED	10
IV.	LEGAL PRINCIPLES.....	11
<i>A.</i>	<i>Enablement, Written Description, and Indefiniteness.....</i>	<i>11</i>
1.	Claim Enablement.....	11
2.	Written Description Support	11
3.	Indefiniteness.....	13
<i>B.</i>	<i>Invalidity Based on Prior Art</i>	<i>13</i>
1.	Prior Art.....	14
2.	Anticipation.....	15
3.	Obviousness.....	16
4.	Enablement of Prior Art	21
5.	Proposed Substitute Claims.....	22
V.	SUMMARY OF MY OPINIONS.....	23
VI.	“FACTORS” USED IN AUTHENTICATION	24
VII.	THE ’199 PATENT – INNOVATIVE ASPECTS OF PROPOSED SUBSTITUTE CLAIM	
	10 29	
<i>A.</i>	<i>Overview.....</i>	<i>29</i>
<i>B.</i>	<i>Preemptive Enablement.....</i>	<i>31</i>
<i>C.</i>	<i>Authentication Using an Identifier Received from a Remote Source.....</i>	<i>35</i>
VIII.	SCs 10-18 ARE FULLY SUPPORTED BY WRITTEN DESCRIPTION.....	38
<i>A.</i>	<i>Claim Element [10.d]</i>	<i>38</i>
<i>B.</i>	<i>Claim Element [10.e.2]</i>	<i>44</i>
IX.	SCs 10-18 ARE PATENTABLE	47

<i>A.</i>	<i>SCs 10-18 Are Clear, Not Indefinite</i>	<i>47</i>
1.	Claim Element [10.d]	47
2.	Claim Element [10.g]	49
X.	SCs 10-18 ARE PATENTABLE – NOT OBVIOUS	53
<i>A.</i>	<i>Key Elements of Proposed Substitute Claim (SC) 10</i>	<i>53</i>
<i>B.</i>	<i>Grounds Based on Jarrell</i>	<i>53</i>
<i>C.</i>	<i>Grounds Based on Pasko</i>	<i>56</i>
<i>D.</i>	<i>Grounds Based on Viggiano and Gong637</i>	<i>62</i>
<i>E.</i>	<i>Petitioners’ Asserted Grounds</i>	<i>63</i>
XI.	CONCLUSION	64

List of Patent Owner Exhibits

Exhibit No.	Description
EX2001	Declaration of Nikolaos Papanikolopoulos, Ph.D., in support of First Motion to Amend
EX2002	U.S. Patent Application No. 15/598,303 (from which U.S. Patent No. 10,249,199 issued) (annotated to include page and line nos.) (the “’303 App.”)
EX2003	U.S. Provisional Patent Application No. 62/309,838 (the “’838 Prov.”)
EX2004	Curriculum Vitae of Dr. Nikolaos Papanikolopoulos
EX2005	Second Declaration of Nikolaos Papanikolopoulos, Ph.D.
EX2006	Declaration of June Munford
EX2007	Curriculum Vitae of June Munford
EX2008	NIST, Digital Signature Standard (DSS), Federal Information Processing Standards (FIPS) Publication 186-4 (2013), <i>available at</i> https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
EX2009	NIST, Electronic Authentication Guideline, Special Publication 800-63-2 (2013), <i>available at</i> https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
EX2010	Carullo, Giuliana, Filomena Ferrucci, and Federica Sarro. "Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment." <i>Information Systems: Crossroads for Organization, Management, Accounting and Engineering: ItAIS:</i>

Exhibit No.	Description
	<i>The Italian Association for Information Systems</i> . Heidelberg: Physica-Verlag HD (2012). 145-153.
EX2011	Lin, Han-Yu, et al. "Construction of a Taiwan biodiversity genetic database in cloud environments." <i>2012 International Symposium on Biometrics and Security Technologies</i> . IEEE (2012).
EX2012	Wee, Oh Khoon. <i>Wireless Network Security: Design Considerations for an Enterprise Network</i> . Diss. MSc. thesis, Naval Postgraduate School Monterey (2004), <i>available at</i> https://apps.dtic.mil/sti/pdfs/ADA429868.pdf
EX2013	Yung, Moti. "On the evolution of user authentication: Non-bilateral factors." <i>International Conference on Information Security and Cryptology</i> . Berlin, Heidelberg: Springer Berlin Heidelberg (2007).
EX2014	PCT Pub. No. WO 2013/101894, Secure User Authentication for Bluetooth Enabled Computer Storage Devices to Weber, Mark et al. (2013).
EX2015	NIST, Digital Signature Standard (DSS), Federal Information Processing Standards (FIPS) Publication 186-4 (2013), <i>available at</i> https://web.archive.org/web/20130809192033/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
EX2016	NIST, Electronic Authentication Guideline, Special Publication 800-63-2 (2013), <i>available at</i> https://web.archive.org/web/20140330034434/http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Exhibit No.	Description
EX2017	A library catalog MARC record for <i>Information Systems: Crossroads for Organization, Management, Accounting and Engineering: ItAIS: The Italian Association for Information Systems</i> , available from Ohio University Library at https://ohiolink-ou.primo.exlibrisgroup.com/discovery/fulldisplay?context=L&vid=01OHIOLINK_OU:OU&search_scope=LibALICE&tab=LibraryCatalog&lang=en&docid=alma9926179331308506
EX2018	Carullo, Giuliana, Filomena Ferrucci, and Federica Sarro. "Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment.", available at https://web.archive.org/web/20200113202746/http://www0.cs.ucl.ac.uk/staff/F.Sarro/resource/papers/B2%20e%20C11_CameraReady.pdf .
EX2019	A library catalog MARC record for <i>2012 International Symposium on Biometrics and Security Technologies</i> , available from Penn State University Library at https://catalog.libraries.psu.edu/catalog/14769967
EX2020	Lin, Han-Yu, et al. "Construction of a Taiwan biodiversity genetic database in cloud environments." <i>2012 International Symposium on Biometrics and Security Technologies</i> . IEEE (2012), as sourced from the Penn State University Library's collection.
EX2021	Wee, Oh Khoon. <i>Wireless Network Security: Design Considerations for an Enterprise Network</i> . Diss. MSc. thesis,

Exhibit No.	Description
	Naval Postgraduate School Monterey (2004), <i>available at</i> https://calhoun.nps.edu/entities/publication/afc87d79-8370-45b9-b8f6-c30859026220
EX2022	An Internet Archive upload record of <i>Wireless Network Security: Design Considerations for an Enterprise Network</i> , <i>available at</i> https://archive.org/details/wirelessnetworks109451246/page/n1/mode/2up
EX2023	A library catalog MARC record for <i>Lecture Notes in Computer Science</i> , <i>available from Penn State University Library at</i> https://catalog.libraries.psu.edu/catalog/51632820
EX2024	Yung, Moti. "On the evolution of user authentication: Non-bilateral factors." <i>International Conference on Information Security and Cryptology</i> . Berlin, Heidelberg: Springer Berlin Heidelberg (2007), <i>as sourced from the Penn State University Library's collection</i> .
EX2025	Merriam-Webster Dictionary, Definition of "preempt," as obtained from https://web.archive.org/web/20150911233241http://www.merriam-webster.com/dictionary/preempt

I, Nikolaos Papanikolopoulos, of Minneapolis, Minnesota, declare that:

I. INTRODUCTION

1. I have been retained by Patent Owner Airspace Defense, Inc. in this *inter partes* review (IPR) proceeding number IPR2025-00530, filed by Petitioners Axon Enterprise, Inc. and Dedrone Holdings, Inc. I understand that this IPR proceeding relates to U.S. Patent No. 10,249,199 (the '199 patent).

2. I was asked to provide my objective, independent analysis of the '199 patent in view of the prior art references cited in the Petition and to provide my opinion regarding the allegations in the Petition and substitute claims proposed by Patent Owner. To this end, I provided a declaration (EX2001) (the "Initial Declaration"), setting forth my opinions. I incorporate the Initial Declaration herein, by reference, in its entirety.

3. I am further asked to provide my objective, independent analysis of the '199 patent and the proposed substitute claims in view of Petitioners' Opposition to Patent Owner's Motion to Amend and the prior art references cited in the Opposition, and to provide my opinions regarding the allegations in the Opposition. My response is set forth herein in this Second Declaration.

4. I have based my opinions on the information available to me as of the date of this declaration. I understand that additional information may become available after this declaration is submitted. If I become aware of additional

information following my submission of this declaration I may, if I am permitted, offer additional opinions (including by amending and/or supplementing this declaration) taking into account such new information.

5. I am not currently, nor have I ever been, an employee of Airspace Defense, Inc., its predecessors, subsidiaries, parent organizations, or affiliates. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent working on this IPR. I will not receive any added compensation based on the outcome of this or any other IPR, or any other proceeding, involving the '199 patent.

II. COMPENSATION

6. I am being compensated as an expert witness in this case at my standard hourly rate in addition to out-of-pocket expenses. I have received no additional compensation for my work on this matter and my compensation does not depend, and has not ever depended in any way, on my opinion as expressed in this declaration and in any testimony that I may give, or on the outcome of this matter. I have no financial stake in Airspace Defense, Inc., its predecessors, subsidiaries, parent organizations, or affiliates, the '199 patent, or the outcome of this IPR or any other matter involving the '199 patent.

III. MATERIALS CONSIDERED

7. In formulating my opinions, I have relied upon my training, knowledge, and experience that are relevant to the '199 patent. I have also considered the '199 patent, patent applications identified in the priority claim of the '199 patent, and its file history. In addition, I have reviewed the Petition ("Pet.") and attached exhibits, including the first declaration by Dr. Chowdhary (EX1003) and the prior art cited by Petitioners. Moreover, I have considered the Board's Institution Decision, Patent Owner's Motion to Amend (MTA), and substitute claims that were initially proposed by Patent Owner in the MTA.

8. Additionally, I have reviewed Petitioner's Opposition ("Opp.") to the MTA, the second declaration by Dr. Chowdhary, the new prior art cited by Petitioners. I also reviewed transcripts of my own deposition, and the Preliminary Guidance ("PG") that the Board provided.

9. Furthermore, I have reviewed Patent Owner's Revised Motion to Amend (RMTA), substitute claims that were proposed by Patent Owner in the RMTA, the third declaration by Dr. Chowdhary, additional new prior art cited by Petitioners.

10. For the sake of convenience and quick reference, I have reproduced above updated Patent Owner's Exhibit List, listing some of the materials that I considered.

IV. LEGAL PRINCIPLES

11. I am not an attorney. I have been asked to provide opinions on patentability of the claims challenged by Petitioners and substitute claims proposed by Patent Owner. To this end, I relied on certain legal principles that were provided to me by counsel and that are summarized below.

A. Enablement, Written Description, and Indefiniteness

1. Claim Enablement

12. I am informed by Counsel and understand that 35 U.S.C. §112(a), requires the patent disclosure as filed to be full and clear so as to enable a POSITA to make and use the invention. I am further informed by Counsel and understand that the Federal Circuit has interpreted the statutory requirement to mean that a POSITA should be able to make and use the invention without “undue experimentation.” *In re Wands*, 858 F.2d 731, 737 (Fed. Cir. 1988). The Court stated that a “patent need not disclose what is well known in the art,” and that some experimentation may be necessary. *Id.* at 735, 737. I am informed by Counsel and understand that what is “undue” may be determined via an eight-factor analysis. *Id.* at 737.

2. Written Description Support

13. Moreover, I am informed by Counsel and understand that the specification reasonably conveys to a POSITA “that the inventor had possession of

the claimed subject matter.” *Ariad Pharmaceuticals, Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). To show possession, “the specification must describe an invention understandable to [an] skilled artisan and show that the inventor actually invented the invention claimed.” *Id.* “A ‘mere wish or plan’ to obtain the claimed invention is not sufficient.” *Novozymes A/s v. DuPont Nutrition Biosciences APS*, 723 F.3d 1336, 1346 (Fed. Cir. 2013). The test of sufficiency of written description “requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art.” *Ariad*, 598 F.3d at 1351.

14. I am also informed by Counsel and understand, however, “it is unnecessary to spell out every detail of the invention in the specification; only enough must be included to convince a person of skill in the art that the inventor possessed the invention and to enable such a person to make and use the invention without undue experimentation.” *LizardTech, Inc. v. Earth Resource Mapping, Inc.*, 424 F.3d 1336, 1345 (Fed. Cir. 2005). Moreover, a “claim will not be invalidated on section 112 grounds simply because the embodiments of the specification do not contain examples explicitly covering the full scope of the claim language.” *Id.*; see *Flash-Control, LLC v. Intel Corporation*, Case No. 2020-2141 at 10 (“A patent owner cannot show written description support by picking and choosing claim

elements from different embodiments that are never linked together in the specification”) (Fed. Cir. 2021) (nonprecedential).

15. In this regard, I am informed by Counsel and understand that in *Union Oil*, “[r]ather than reciting a recipe of specific ingredients,” claims to certain “gasoline compositions” in that case “defined the claimed gasoline compositions in terms of various chemical and physical properties,” and were found to have “adequate written description support.” *Novozymes*, 723 F.3d 1347-48 (citing *Union Oil Co. of California v. Atlantic Richfield Co.*, 208 F.3d 989 (Fed. Cir.2000)).

3. Indefiniteness

16. Additionally, I am informed by Counsel and understand that 35 U.S.C. §112(b), requires a patentee to present claim(s) that particularly point out and distinctly claim the subject matter which the inventor(s) regard as the invention. I am informed by Counsel and understand that the Supreme Court has interpreted this requirement to mean that a claim, “read in light of the specification ... and the prosecution history,” must “inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 US 898 (2014).

B. Invalidity Based on Prior Art

17. I am informed by Counsel and understand that each claim of an issued patent is presumed to be valid. In an IPR proceeding, a party challenging the

validity of a patent claim, whether an issued claim or a proposed substitute claim, must present a preponderance of the evidence to demonstrate invalidity of that claim.

1. Prior Art

18. I am informed by counsel and understand that in an IPR proceeding, a Petitioner can only rely upon a patent or other publication as prior art. I also understand that a particular patent may claim priority to one or more earlier filed patent applications, and that subject to meeting certain conditions, the effective filing date of that particular patent can be the actual filing date of the earliest patent application in the priority claim of that particular patent. I am also informed by Counsel and understand that the earliest priority date of a patent is the effective filing date of that patent.¹

19. I understand further that with respect to a challenged patent, a U.S. or foreign patent may qualify as prior art if the date of issuance of the patent is prior to the effective filing date of the challenged patent. A particular U.S. patent that issued after the effective filing date of a challenged patent may qualify as prior art

¹ I am informed by Counsel that in certain cases, if the effective filing date is earlier than March 16, 2013, the earliest priority date of that patent may be the date of invention of the claimed invention of that patent.

to the challenged patent if the effective filing date of that particular patent is earlier than the effective filing date of the challenged patent.

20. I also understand that a printed publication, such as an article published in a magazine, academic journal, conference proceedings, or trade publication, or U.S. or foreign published patent application qualifies as prior art to a challenged patent if the date of publication of that printed publication is prior to the effective filing date of the challenged patent. Additionally, I am informed by Counsel and understand that to qualify as prior art, a reference, whether a patent, published patent application, or another printed publication, must contain an enabling disclosure that allows one of ordinary skill to practice the claims without undue experimentation.

2. Anticipation

21. I understand that, once a claim of a challenged patent has been properly construed, the next step in determining whether that claim is anticipated by a prior art reference under 35 U.S.C. § 102 requires a comparison of the properly construed claim language to the prior art reference on a limitation-by-limitation basis.

22. I understand that a prior art reference “anticipates” a challenged claim, and therefore renders the claim invalid, if all elements of the claim are disclosed in that prior art reference, either expressly or inherently (i.e., necessarily

present), arranged in the same way as in the claim. I understand that, for inherent anticipation, it is required that the missing descriptive material is necessarily present in the prior art reference, and not merely probable.

23. I also understand that to anticipate a challenged claim, an allegedly anticipatory prior art reference must provide a disclosure that enables the challenged claim. I understand an enabling disclosure describes the invention of the challenged claim in sufficient detail that would allow a POSITA to make and use that invention without undue experimentation.

24. I understand that for the purposes of an IPR proceeding, a patent claim is anticipated if there is proof that, more than one year before the priority date of that claim, the claimed invention was: patented anywhere in the world or described in a printed publication anywhere in the world. This I am informed by Counsel is called a statutory bar.

25. I have written this declaration with the understanding that, in an IPR, anticipation must be shown by a preponderance of the evidence. I understand that a preponderance of the evidence means that it is more likely than not that the prior art reference discloses all of the elements of a challenged claim.

3. Obviousness

26. I am informed by Counsel and understand that even if a challenged claim is not anticipated, it may still be invalid pursuant to 35 U.S.C. § 103 as

obvious, if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA.

27. I understand that a POSITA provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the challenged claim, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations (also called objective indicia of non-obviousness).

28. I am further informed by Counsel and understand that a claim is not proved obvious merely by demonstrating that each of the elements was independently known in the prior art. I understand that many inventions rely on known building blocks, and that claimed inventions, often of necessity, can be combinations of what was already known. I understand that it is therefore important to identify whether a reason existed at the time of the invention that would have prompted a POSITA to combine such known elements in the way the claimed invention does. Such reasons are typically described as the motivation to combine two or more prior art references.

29. I understand that an obviousness evaluation can be based on a combination of several prior art references. I understand that the prior art references themselves may sometimes provide a suggestion, motivation, or reason to combine, but at other times the nexus linking two or more prior art references can be based on the ordinary understandings available to a POSITA. I further understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

30. I am also informed by Counsel and understand that the use of hindsight must be avoided when considering whether the alleged invention would have been obvious to a POSITA. In assessing obviousness, I have been instructed to consider the distortion caused by hindsight bias, guard against slipping into the use of hindsight, to be cautious of arguments that rely upon after-the-fact reasoning, and to avoid the temptation to read into the prior art the teachings of the invention in issue.

31. I further understand that secondary considerations of non-obviousness (also known as objective indicia of non-obviousness) may include: (1) a long felt but unsolved need; (2) commercial success; (3) unexpected results; (4) industry praise; (5) licensing; and (6) copying by others. I also understand that there must be a relationship or nexus between any such secondary considerations and the

claimed invention. Where the offered secondary consideration results from something other than what is both claimed and novel in a challenged claim, there is no nexus to the merits of the claimed invention.

32. I understand that a nexus is presumed where the secondary considerations are tied to a particular product which: (i) embodies the claimed invention and (ii) is coextensive with the claimed invention. In analyzing whether a product is coextensive with the claimed invention, I understand that there is no requirement for a perfect correspondence between the claims and the product, and that the presumption of a nexus can still apply when unclaimed features present in the product amount to nothing more than additional insignificant features.

33. I further understand that Patent Owner bears the burden of demonstrating that the relevant secondary indicia are attributable to the claimed invention, as opposed to other economic and commercial factors unrelated to the technical quality of the patented subject matter. I also understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination. Additionally, I understand that, as a safeguard against hindsight bias, all secondary considerations of non-obviousness must be considered prior to reaching an obviousness conclusion.

34. It is further my understanding, as informed by Counsel, that a proper obviousness analysis focuses on what was known or obvious to a POSITA, not just

Patent Owner. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the challenged patent can provide a reason for combining the elements in the manner claimed.

35. I understand that whether a prior art reference “teaches away” from the claimed invention is a fact to be considered in determining obviousness. I understand that it is improper to combine references where the references teach away from their combination. I understand, however, that the nature of the teaching is highly relevant and must be weighed in substance; a challenged claim may be obvious over a combination of prior art teachings even if one of those teachings has been described as somewhat inferior to some other teachings. Furthermore, I understand that the prior art’s mere disclosure of more than one alternative does not constitute a teaching away from a particular alternative when such disclosure does not criticize, discredit, or otherwise discourage the use of that alternative.

36. I understand that, in an IPR proceeding, obviousness must be proven by a preponderance of the evidence such that a POSITA at the time of the alleged invention would have had a reason (or reasons) for combining the teachings of those prior art references to achieve the claimed invention, and that the POSITA would have had a reasonable expectation of success of achieving the claimed invention by combining those teachings.

4. Enablement of Prior Art

37. I am informed by Counsel and understand that to “render a claim obvious, the prior art, taken as a whole, must enable a skilled artisan to make and use the claimed invention.” *Raytheon Technologies v. General Electric Co.*, 993 F.3d 1374, 1380 (Fed. Cir. 2021). A “prior art reference asserted under § 103 does not necessarily have to enable its own disclosure, i.e., be ‘self-enabling,’ to be relevant to the obviousness inquiry.” *Id.* “But even though a non-enabling reference can play a role in an obviousness analysis, the evidence of record must still establish that a skilled artisan could have made the claimed invention.” *Id.* at 1381.

38. I am also informed by Counsel and understand that “[e]nablement requires that the prior art reference must teach one of ordinary skill in the art to make or carry out the claimed invention *without undue experimentation*.” *Elan Pharmaceuticals v. Mayo Foundation*, 346 F.3d 1051, 1054 (Fed. Cir. 2003) (internal quotation marks omitted). “[W]hat constitutes undue experimentation” regarding the disclosure of a prior art reference can be determined using the eight factors described in *In re Wands*.” *Id.* at 1054-55 (citing *In re Wands*, 858 F.2d 731 (Fed. Cir. 1988)).

39. I am further informed by Counsel and understand that in *Raytheon*, it was an error to “focus[] only on whether [a skilled artisan] is provided with

sufficient parameters in [a prior art reference] to determine, without undue experimentation,” the claimed limitation, “rather than determining whether [that prior art reference] enabled a skilled artisan to make and use the claimed invention.” *Raytheon*, 993 F.3d at 1380. A prior art reference’s “self-enablement (or lack thereof) is not only relevant to the enablement analysis, ... it is dispositive” when “no [] other evidence [is] presented” “to establish that a skilled artisan could have made the claimed” invention. *Id.* at 1382.

5. Proposed Substitute Claims

40. I am informed by Counsel and understand that in a motion to amend, Patent Owner may cancel any challenged claim or propose a reasonable number of proposed substitute claims for each challenged claim. 35 U.S.C. § 316(d)(1). I am also informed by Counsel and understand that there is a rebuttable presumption that a reasonable number of proposed substitute claims per challenged claim is one. 37 C.F.R. § 42.121(a)(3).

41. I am also informed by Counsel and understand that per the applicable rules, a motion to amend may be denied if it does not respond to a ground of unpatentability involved in the trial. 37 C.F.R. § 42.121(a)(3). I am further informed by Counsel and understand that the “rule does not require ... that every word added to or removed from a claim in a motion to amend be solely for the purpose of overcoming an instituted ground,” and that additional modifications

may be included. *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 15 (Information and Guidance on Motions to Amend) at 5-6.

42. Additionally, I am informed by Counsel and understand that no proposed substitute claim may enlarge the scope of the claims of the challenged patent. 35 U.S.C. § 316(d)(3); 37 C.F.R. § 42.121(a)(2)(ii). Finally, I am informed by Counsel and understand that no proposed substitute claim may introduce new subject matter. 35 U.S.C. § 316(d)(3); 37 C.F.R. § 42.121(a)(2)(ii).

V. SUMMARY OF MY OPINIONS

43. Petitioners have challenged the proposed independent substitute claim 10 on various grounds. This claim recites that an “identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system,” where the discrimination system includes the unmanned aerial system. The proposed substitute claim 10 also recites that “the identification system is configured to ... verify an authenticity of the first identifier using the second identifier.” Petitioners appear to have misunderstood the transmission and function of the two identifiers. As a result of this misunderstanding, their assertions and arguments— regarding a purported lack of written description support, indefiniteness, and invalidity in view of prior art, fail.

44. The proposed substitute claim 10 also recites that “the disruption system is preemptively enabled based on the received aerial system identifier signal.” Petitioners appear to have also misunderstood the “preemptively enabled” limitation. As a result of this misunderstanding, their arguments regarding the indefiniteness of this claim limitation fail.

45. Because the proposed independent substitute claim 10 is valid, all of its dependent claims are also valid.

VI. “FACTORS” USED IN AUTHENTICATION

46. Before the priority date of the ’199 patent (March 17, 2016), the meaning of “second factor” used in an authentication system/process was well-understood. For example, the National Institute of Standards and Technology (NIST) defined “multi-factor” as used in multi-factor authentication (MFA) as:

Multi-Factor	A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.
--------------	---

EX2009² at 11. NIST describes “tokens” as:

² Archived NIST Technical Series Publication – NIST Special Publication (SP) 800-63-2, “Electronic Authentication Guidance,” (August 2013 – Withdrawn June 22, 2017)

4.3. Tokens

The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- *Something you know* (for example, a password)
- *Something you have* (for example, an ID badge or a cryptographic key)
- *Something you are* (for example, a fingerprint or other biometric data)

Multi-factor authentication refers to the use of more than one of the factors listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors. (As discussed in Section 4.1, other types of information, such as location data or device identity, may be used by an RP or Verifier to reject or challenge a claimed identity, but they are not considered authentication factors.)

Id. 20.

47. Thus, a “factor” used for authentication is one of: “something you know,” “something you have,” or “something you are.” The use of “more than one ... factor[]” is not simply the use of more than one *instances* of just one of the factors, such as two passwords instead of one. Rather, it is the use of at least two or all three of the above-identified factors. *See, e.g.,* EX2014,³ ¶40 (“where a user desires stronger authentication, two-factor authentication, where both the ‘something you have’ and ‘something you know’ authentication factors are

³ PCT Pub. No. WO 2013/101894, Secure User Authentication for Bluetooth Enabled Computer Storage Devices.

required, may be utilized”); EX2012⁴ (“Multi-factor authentication adds strength to current authentication mechanisms by adding the attributes of ‘something you have’ to the traditional ‘something you know’ (i.e. passwords) schemes.”).

48. Accordingly, if one identifier used for authentication is “something you know,” another identifier functioning as a “second factor,” cannot also be something else that you know; it must be “something you have” or “something you are.” An identifier associated with a device, such as a medium access control (MAC) address, an International Mobile Equipment Identity (IMEI) number, when used for device authentication, belong to the “something you have” category of authentication factors. *See* EX2011⁵ (disclosing “a specific MAC address” as an example of “[s]omething you have”); EX2013⁶ (describing a “mac address” as “Something Embedded in the User’s Computing Environment,” that “can [] be

⁴ Wee, O. K. (2004). *Wireless Network Security: Design Considerations for an Enterprise Network* (Doctoral dissertation, MSc. thesis, Naval Postgraduate School Monterey).

⁵ Lin, H. Y., Chen, C. M., Chen, Y. L., Chang, Y. H., & Pai, T. W. (2012, March). Construction of a Taiwan biodiversity genetic database in cloud environments. In *2012 International Symposium on Biometrics and Security Technologies* (pp. 108-112). IEEE.

⁶ Yung, M. (2007, August). On the evolution of user authentication: Non-bilateral factors. In *International Conference on Information Security and Cryptology* (pp. 5-10). Berlin, Heidelberg: Springer Berlin Heidelberg.

thought of as ‘something the user has,’”); *see also* EX2010⁷ at 3, 4 (describing an “authentication scheme ... using a smartphone as unique hardware token (something you have),” and noting that an “IMEI (International Mobile Equipment Identity)” is a “unique identifier[] associated to mobile phone”).

49. While a MAC address / ID, an IMEI number, a serial number, or a government registration number assigned to a device can be known by the user / owner of that device, these entities are not known in the same sense as a password is known, or an answer to a question “what was your first car” is known by an authentic user, and are expected to be known only by the authentic user. Rather, they are attributes *assigned* to a device and thus, each of these is generally understood as “something you have.”

50. To the extent encryption keys are used in user/device authentication, such keys also belong to the category of “something you have.” For example, NIST states:

⁷ Carullo, G., Ferrucci, F., & Sarro, F. (2012). Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment. In *Information Systems: Crossroads for Organization, Management, Accounting and Engineering: ItAIS: The Italian Association for Information Systems* (pp. 145-153). Heidelberg: Physica-Verlag HD.

The secrets contained in tokens are based on either *public key pairs* (asymmetric keys) or *shared secrets*.

A *public key* and a related private key comprise a public key pair. The *private key* is

Shared secrets stored on tokens may be either *symmetric keys* or passwords. While they can be used in similar protocols, one important difference between the two is how they relate to the subscriber. While symmetric keys are generally stored in hardware or software that the Subscriber controls, passwords tend to be memorized by the Subscriber. As such, keys are something the Subscriber has, while passwords are something he or she knows. Since passwords are committed to memory, they usually do not have as many possible values as cryptographic keys, and, in many protocols, are vulnerable to network attacks that are impractical for keys. Moreover the entry of passwords into systems (usually through a keyboard) presents the opportunity for very simple keyboard logging attacks, and it may also allow those nearby to learn the password by watching it being entered. Therefore, keys and passwords demonstrate somewhat separate authentication properties (something you have rather than something you know). However, when using either public key pairs or shared secrets, the Subscriber has a duty to maintain exclusive control of his or her token, since possession and control of the token is used to authenticate the Claimant's identity. Token threats are discussed more in Section 6.2.

EX2008 at 21; *see id.* at 20 (listing “a cryptographic key” as an example of “Something you have”).

51. The '199 patent uses the term “second factor” in the same manner as discussed above. In particular, the '199 patent states:

[T]he aerial system 100 can include a first and second identifier, transmitted by a first and second identifier transmission system, respectively, wherein the second identifier can function as a backup identifier (e.g., in case the primary identifier transmission system is inoperable), *a second factor identifier* for the aerial system 100 (e.g., as a secondary authenticator for the aerial system *to prevent tampering and/or identifier reproduction*).

EX1001, 2:57-67.

52. A “second factor” can provide enhanced security because it can prevent identifier reproduction. “[I]dentifier reproduction,” also known as spoofing, occurs when a rogue entity, e.g., a rogue UAV, steals an identifier of an authorized entity (e.g., an authorized UAV) and passes that identifier as its own. The likelihood that the rogue UAV can also successfully steal a “second factor” identifier of the same authorized UAV – an identifier of a distinct kind – is rather low. Thus, when a second factor is also used for authentication, at least one of the two factors can detect if the identifiers provided by an entity / UAV are not authentic, which provides protection against identifier reproduction / spoofing. The likelihood of such a detection increases even further, if the second factor identifier is not received from the UAV (whether authorized or rogue) but from a different remote system.

VII. THE ’199 PATENT – INNOVATIVE ASPECTS OF PROPOSED SUBSTITUTE CLAIM 10

A. Overview

53. I discussed the innovative aspects of the ’199 in my Initial Declaration. EX2001, § VIII.C. Upon reviewing Petitioners’ Opposition (Opp.) to Patent Owner’s Revised Motion to Amend (RMTA), and the Third Declaration by Dr. Chowdhary (EX1024), it appears to me that the Petitioners have misunderstood certain key innovative aspects disclosed in the ’199 patent and claimed in the

proposed independent substitute claim (hereinafter, “SC”) 10. I therefore describe these key aspects below.

54. The ’199 patent discloses and claims a “discrimination system” that can “discriminate between authorized and unauthorized aerial systems,” and can “treat authorized aerial systems differently from unauthorized” ones, e.g. “leave alone vs. interdict, respectively.” EX1001, 2:42-47. To accomplish the goal of effective discrimination, the ’199 patent describes a discrimination system 110 that, along with a disruption system 105, also includes an identification system 111 and a permissions module 103. *See id.*, 2:5-10, FIG. 1.

55. The disruption system 105 may “include a launching system 303 and an interdiction module 304 ... to intercept, then interdict, the aerial system 100.” *Id.* 10:41-44, 10:56-59, FIGS. 1, 3. The “disruption system 105 can include a jamming system, an electromagnetic disruption system , a buckshot system (e.g., a system that fires buckshot), an ablation system , a projectile net system , or any other suitable mechanism capable of interfering with aerial system operation.” *Id.* 10:59-64.

56. A powerful disruption system such as the one that the ’199 patent describes is beneficial only if it is reliable. Reliable in this context means that the disruptive action is taken as soon as possible, but not against genuine, authorized entities (though some errors, as long as they are within an acceptable error margin,

may be unavoidable). Considering the high-speed movement of aerial vehicles in a three-dimensional space, a reliable operation depends at least part on how quickly the disruption system can activate. If the system response is slow, an unauthorized UAV may be able to evade the disruption system, or complete an unauthorized mission, such as taking pictures of private grounds while in the restricted airspace.

57. Reliability also means that the system identifies (within an acceptable error margin) all unauthorized UAVs, so that the likelihood of an unauthorized UAV entering and/or remaining in a restricted airspace is minimized. To address the first reliability aspect, the '199 patent describes and claims a preemptively enabled disruption system. Regarding the second reliability aspect, the '199 patent describes and claims an authentication process that uses two identifiers that are received from two different sources.

B. Preemptive Enablement

58. The commonly understood meaning of the word “preemptively” is “to seize upon to the exclusion of others.” EX2025. Preemption also means “to prevent from happening or taking place,” i.e., to “forestall” or to “preclude.” *Id.* The '199 patent discloses a preemption process that is consistent with this well understood meaning of preemptive.

59. In general, the '199 patent is directed to techniques for protecting airspace, and describes that its

method for aerial system discrimination and action includes ... determining whether the aerial system parameters are permitted based on the set of permissions 203. Further, if the aerial system is not permitted, enabling a disruption system 204, and disrupting the operation of the aerial system 205.

EX2002, 26:9-15, FIG. 2; EX1001, 13:61-14:4.

60. Additionally, the specification states:

Controlling disruption system operation can include: *selecting* a disruption system *operation mode based on the determined aerial system permission* and controlling the disruption system operation to meet the selected mode. Selecting a disruption system operation mode based on the determined aerial system permission preferably includes: selecting an *enabled operation mode in response to aerial system classification as not permitted* (e.g., prohibited) and selecting a disabled operation mode in response to aerial system classification as permitted.

EX2002, 36:8-14; EX1001, 18:63-19:6.

61. While the disruptive system may be enabled and the detected aerial system's operation may be disrupted *immediately* upon determining that the aerial system is not permitted, the '199 patent also states that "the disruption system operation can be *otherwise controlled*." EX2002, 37:8; EX1001, 19:32-33. In particular:

The method can optionally include contacting the aerial system pilot *prior to disruption system activation*. Contacting the user can

include: presenting the user with a notification (e.g. sending, displaying, etc.), wherein the notification can notify the user that the aerial system is within restricted airspace, *give the user a warning* (e.g., a *time limit to leave* the restricted airspace), query whether the user is the pilot, or present any other suitable information to the user.”

EX2002, 37:9-18; EX1001, 19:32-47.

62. Thus, upon determining that a detected aerial system did not provide an identifier, or is not authentic, or is not permitted, the disruption system would be enabled or activated, but “*prior* to disruption system activation” and before disrupting the operation of the aerial system 205, the discrimination process may exercise one or more less aggressive options and actions, such as allowing the aerial system to establish authenticity from a pilot, allowing the aerial system to leave the restricted airspace, etc.

63. In describing a pre-emptively enabled system, however, the ’199 patent states:

[C]ertain scenarios may require the disruption system 105 to be ready to engage on short notice. As depicted in FIGURE 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.). Such a configuration would minimize any delays associated with powering on the disruption system 105 and thus allow the system to respond to fast moving aerial systems 100.

EX2002, 36:20-37:3 (noting that disruption system operation mode can be otherwise selected); EX1001, 19:14-25, FIG. 5. Thus, when one of the above-identified conditions is met, the disruption system is pre-emptively enabled, without exercising the less aggressive options that the '199 patent describes such as contacting the user of the aerial system.

64. The '199 patent's system thus seizes upon the aggressive option of taking a disruptive action to the exclusion of other less aggressive options, such as communicating with the aerial system, allowing it to leave airspace, etc. *See* 2025. Thus, the less aggressive options are forestalled or precluded. *See id.* This may rapidly prevent an unauthorized aerial vehicle from continuing its operation in a restricted airspace, which the aerial vehicle could have accomplished over a longer time period if one of the less aggressive options were chosen such as communicating with the aerial system before enabling the disruption system.

65. In terms of reliable operation, the preemptive system performs the following tradeoff. On one hand, there is a risk that disruptive action may be taken against an aerial vehicle that was in fact authorized, where the authorized status of the aerial vehicle was not determined (e.g., due to an error in the records, error in transmission, etc.). This risk could be sidestepped by taking one of the less aggressive options instead such as communicating with the aerial system before enabling the disruption system. On the other hand, there is a risk that while taking

time to exercise these less aggressive options including attempting to communicate with the aerial system, a rogue aerial vehicle may complete its unauthorized actions and/or may evade the disruption system.

C. Authentication Using an Identifier Received from a Remote Source

66. To be effective in protecting a restricted airspace, the '199 patent describes a particular manner of maximizing the likelihood of identifying the unauthorized UAVs. In addition to permissions checking, various embodiments of the '199 patent also feature authenticating the identifier transmitted by a UAV and received by an identification system. To provide effective authentication, the '199 patent describes:

[T]he aerial system 100 can include a *first and second identifier*, transmitted by a first and second identifier transmission system, respectively, wherein the second identifier can function as a backup identifier (e.g., in case the primary identifier transmission system is inoperable), a *second factor identifier* for the aerial system 100 (e.g., as a secondary authenticator for the aerial system to *prevent tampering and/or identifier reproduction*), an identifier for a secondary identification system (e.g., a user device-compatible identifier), or be used in any other suitable manner.

EX2002, 4:15-22, EX1001, 2:57-67.

67. Identifier reproduction, also known as spoofing, occurs when a rogue aerial system (e.g., a UAV X), steals the identifier of an authorized entity (e.g., a

UAV A that is authorized to enter and roam a restricted airspace), and passes off that identifier as its own. Such spoofing can defeat a discrimination system that assumes the received identifier belongs to the aerial system that transmitted it, since the discrimination system will not take disruptive action against the rogue aerial system it thinks that system is associated with the stolen (and permitted) identifier.

68. Protection against identifier reproduction / spoofing can be provided by determining whether the identifier received from a detected UAV is authentic, i.e., by determining whether or not the identifier in fact belong to the UAV that transmitted it. The ‘199 patent’s claimed use of a second identifier helps verify the authenticity of the first identifier received from the UAV because the likelihood of a rogue actor stealing two different identifiers of the same authorized UAV is relatively lower than that of their stealing only one of the identifiers.⁸ Still further protection against identifier reproduction / spoofing can be provided if the two identifiers conform to two different security factors as discussed below.

69. The robustness of the two-factor identifier authentication scheme can be further increased if one of the identifiers is received from a remote system, i.e.,

⁸ It is worth noting that a rogue entity’s theft of two identifiers from two different authentic UAVs would not permit spoofing of either of those two identifiers, since identifiers from two different UAVs cannot authenticate each other.

a trusted system as opposed to both identifiers being received from the UAV itself.

In this case, the rogue UAV cannot manipulate the identifier transmitted by the remote system. To this end, the '199 patent describes:

The aerial system identifier 310 preferably identifies an aerial system 100, and is preferably globally unique, but can alternatively be unique for a geographic region, unique for a period of time, generic, or otherwise related to other aerial system identifiers. The aerial system *identifier 310 is preferably dynamic*, but can alternatively be *static*. Dynamic aerial system identifiers can be generated, re-assigned, calculated (e.g., based on a static identifier and a changing equation; based on changing identifier and a static equation; based on static identifier, a static equation, and a changing factor, such as a timestamp or a GPS coordinate, etc.), or otherwise determined at a predetermined frequency, in response to the occurrence of a trigger event (e.g., upon user reassignment of the identifier transmission system 101 to a different aerial system), or at any other suitable time. The *dynamic aerial system identifier can be generated* on-board the aerial system 100, generated remotely (e.g., *at a remote computing system*, etc.; updated in-flight or when connected to a predetermined communication connection type, etc.), or generated by any other suitable system.

Id. 7:58-8:10.

70. Thus, the '199 patent's disclosure and use of first and second identifiers, where the second identifier can prevent identifier reproduction /

spoofing, and tampering, because it is generated by a remote computing system, can substantially improve the reliability of identifying unauthorized UAVs.

71. SC 10 was amended and directed to the above described innovative features disclosed in the '199 patent.

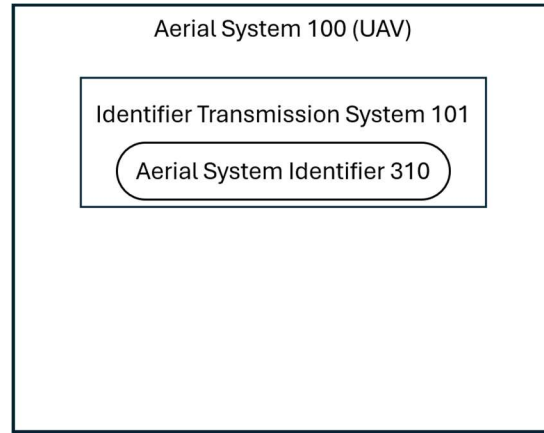
VIII. SCs 10-18 ARE FULLY SUPPORTED BY WRITTEN DESCRIPTION

A. *Claim Element [10.d]*

72. The written description sufficiently discloses the limitations recited in claim element [10.d]. Petitioners argue, however, that the amendments to claim 10, resulting in SC 10, “introduce[] an architectural contradiction.” Opp. at 1; EX1024 (Chowdhary Decl), ¶42. In support of this argument, Petitioners allege there is “[o]nly one source for the transmission of the second identifier: the identifier transmission system itself.” Opp. at 1; EX1024, ¶44. Petitioners further state that “‘aerial system identifier 310’ ... is not described as the claimed second identifier,” and that in disclosing that the “‘dynamic aerial system identifier’ can be generated remotely from the aerial system, the ‘199 patent does not say from where that second identifier is transmitted or from where the identification receiver receives it.” Opp. at 2; EX1024, ¶45.

73. These arguments are erroneous. The specification of the '199 patent discloses an “aerial system 100,” e.g., a UAV, that includes an “identifier transmission system 101,” that “transmit[s an] aerial system identifier 310.”

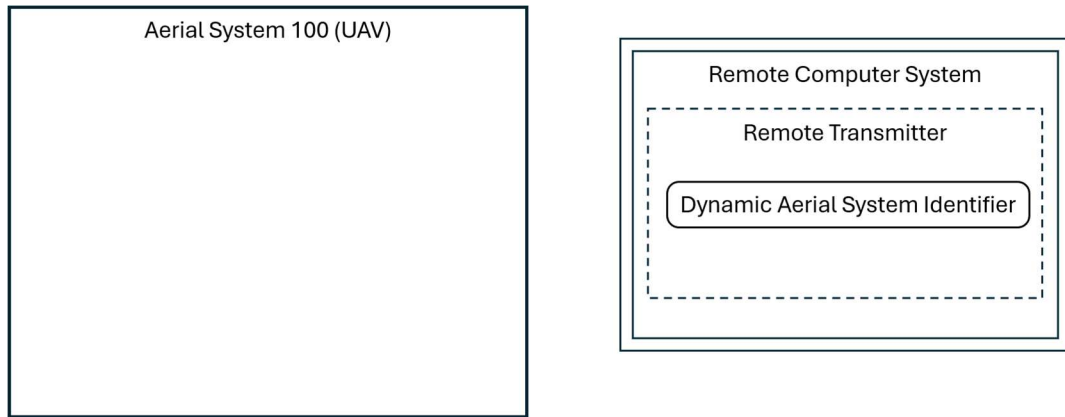
EX2002, 2:18-22; RMTA at 6-8. I have depicted this first embodiment, which I call Embodiment A, in the demonstrative below.



Embodiment A

Demonstrative 1

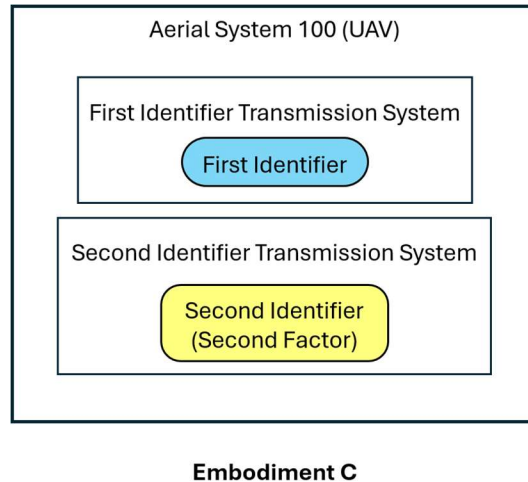
74. The specification also states that “the aerial system identifier 310 is preferably dynamic” but can be static. Moreover, the specification states that the “dynamic aerial system identifier can be generated on-board the aerial system 100, [or] generated remotely [] e.g., at a remote computing system.” EX2002, 14:16-15:2. “[A]erial system identifier signal 300” is received by “the identification receiver 102.” EX2002, 14:6-8. The embodiment per the first option, where the dynamic aerial system identifier is generated on-board, is substantially the same as embodiment A depicted above. In the demonstrative below, I have depicted the embodiment per the second option (called Embodiment B), where the dynamic aerial system identifier is generated at a remote computing system.



Embodiment B

Demonstrative 2

75. Additionally, the specification discloses an embodiment in which “the aerial system 100 can include a first and second identifier, transmitted by a first and second identifier transmitter system, respectively, wherein the second identifier can function as ... a second factor identifier.” EX2002, 4:15-22. I have depicted this embodiment, which I call Embodiment C, in the demonstrative below. Finally, the specification states that “[a]lthough omitted for conciseness, the preferred embodiments include every combination and permutation of various system components.” EX2002, 39:6-9.

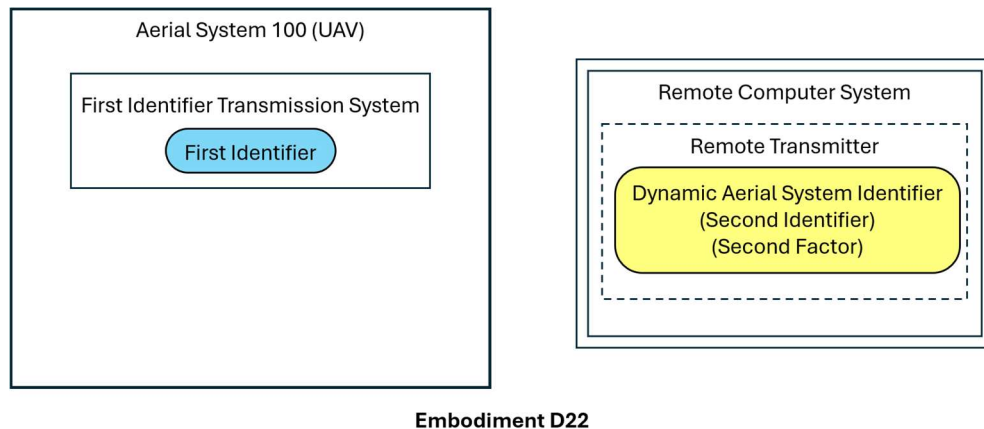


Demonstrative 3

76. Thus, the specification explicitly discloses two embodiments, each transmitting only one aerial system identifier, either from the aerial system (Embodiment A) or from a remote computing system (Embodiment B), and one embodiment, Embodiment C, where two aerial system identifiers are transmitted, both from the aerial system. I am informed by Counsel and understand that the written description analysis is performed “from the perspective of a person of ordinary skill in the art.” *Ariad Pharmaceuticals*, 598 F.3d at 1351. In the context of the ’199 patent, the skill of a POSITA is high. *See* EX2001, ¶52; EX1003, ¶62. A POSITA would have understood that the permutations and combinations of the above-described embodiments are limited because Embodiments A and B cannot be combined because they are mutually exclusive. Additionally, combining Embodiments A and C would not result in a new embodiment because Embodiment C covers Embodiment A.

77. Embodiment C can be varied based on Embodiment B as follows:

- Embodiment D1: both identifiers can be transmitted from a remote computing system;
- Embodiment D21: Only the first identifier is transmitted from a remote computing system; and
- Embodiment D22 (depicted below): Only the second identifier is transmitted from a remote computing system.



Demonstrative 4

78. Embodiments D21 and D22 are virtually indistinguishable; in each case, one identifier is transmitted from the aerial system and another identifier is transmitted from a remote computing system.

79. Thus, with respect to claim element [10.d] the specification of the '199 patent is not a mere wish or simply a speculative plan. *See Novozymes*, 723 F.3d at 1346. Rather, it is an example (Embodiment D22) that readily follows from

explicitly disclosed examples / embodiments. *LizardTech*, 424 F.3d at 1345. These embodiments are directly related to each other because they both describe the transmission of the aerial system’s identifier(s), and Example D22 does not require randomly picking and choosing elements. Rather, the disclosed elements of Embodiment C are logically varied as disclosed in Embodiment B. See *Flash-Control* at 10; *Novozymes*, 723 F.3d 1347-48.

80. I understand that Petitioners also specifically argue that the specification’s disclosure of “generated remotely from the aerial system itself does not identify from where it is transmitted or from where the identification receiver received it.” Opp. at 2. However, the full passage states that “[t]he dynamic aerial system identifier can be generated on-board the aerial system [or] generated remotely (e.g., at a remote computing system, etc.; updated in-flight or when connected to a predetermined communication connection type, etc.).” EX2002, 8:5-10. Moreover, the specification also discloses that the “identification receiver 102, [] functions to receive the aerial system identifier signal 300.” *Id.*, 4:57-59. A POSITA would understand that these passages disclose that the remote computing system—which is outside of the discrimination system—can generate and transmit identifiers and that such identifiers are received by the identification receiver.

81. Indeed it appears that Petitioners’ argument has the effect of improperly rewriting the claim to require that the second identifier be received

directly from the remote computing system. The claim is not so limited. In my opinion, in context of the specification (and particularly the above-discussed passages), a POSITA would understand the claim to encompass identifiers originating *from* the remote computing system, regardless of whether they are transmitted to the identification receiver directly or indirectly (e.g. through the UAV which has “updated in-flight” with the new dynamic ID). Furthermore, in my opinion, the specification’s disclosure of that indirect example is representative of the full scope of the claim. In particular, the issue of how exactly a piece of information would be transmitted from a remote source to the discrimination system’s identification receiver is a matter of a few predictable options (e.g. direct or indirect). Thus, in my opinion, a POSITA reading the disclosed indirect example would recognize the disclosure of the general principle of conveying remotely generated identifiers to the identification receiver.

82. As such, in my opinion, the specification of the ’199 patent fully supports the limitations recited in claim element [10.d].

B. Claim Element [10.e.2]

83. Regarding this claim element, Petitioners argue that “the specification does not disclose that ... an authenticated first identifier of the aerial system identifier signal, is provided to a permission module.” Opp. at 3; EX1024 (Chowdhary Decl), ¶49. In support of this argument, Petitioners acknowledge that

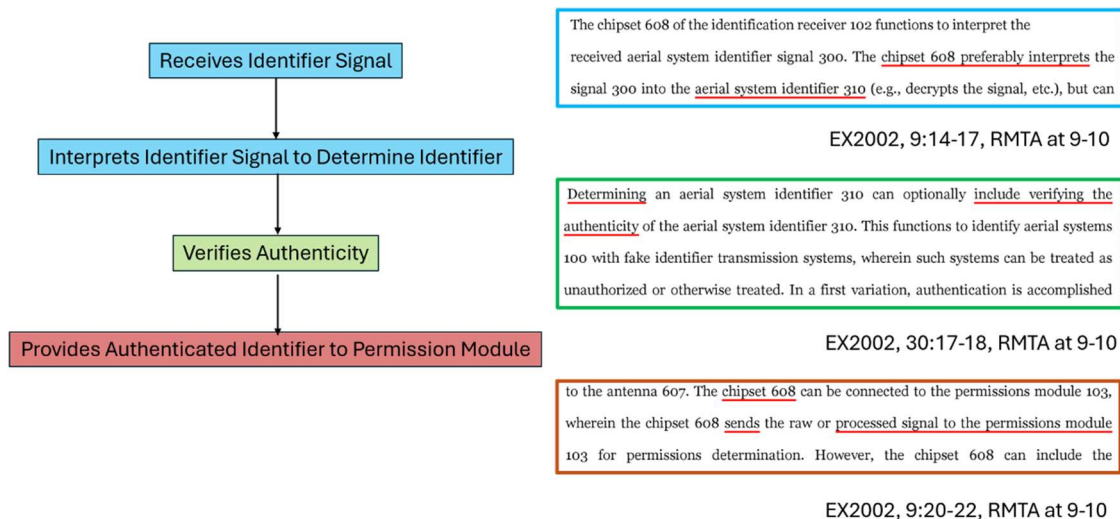
the '199 patent's chipset 608 "sends the 'raw or processed signal to the permissions module 103 for permissions determination," but allege nevertheless that "nowhere does the specification disclose that an authenticated first identifier is provided to the permissions module." EX1024, ¶49. Petitioner also argues that although the '199 patent teaches "an authenticity of the identifier is verified[,] it does not say that any authenticated identifier is provided to the permission module." EX1024, ¶49. These allegations and the arguments are incorrect, as I explain below.

84. The specification states that "identification system 111 can include an identification receiver 102, which functions to receive the aerial system identifier signal 300," and that the "the identification receiver 102" includes a "chipset 608," that "preferably interprets the signal 300 into the aerial system identifier 310." EX2002, 8:16-17, 8:21-23, 9:14-17. Thus, the specification discloses that the chipset 310 can determine the aerial system identifier 310 from a received identification signal 300.

85. The specification further states that "[d]etermining an aerial system identifier 310 can optionally include verifying the authenticity of the aerial system identifier 310." EX2002, 30:17-18. Thus, as part of determining the identifier 310 from the signal 300, the chipset 608 can verify the authenticity of the identifier 310, thereby yielding an authenticated identifier. The specification also states that "chipset 608 can be connected to the permissions module 103, wherein the chipset

608 sends the raw or *processed signal* to the permissions module 103 for permissions determination.” EX2002, 9:20-22. It follows that as the Court found in *LizardTech*, the processed signal 300 includes the determined identifier 310, the authenticity of which is verified, is a detail that a POSITA would have readily understood. *LizardTech*, 424 F.3d at 1345.

86. Thus, in sum, the specification discloses that the chipset 608: (i) receives an identifier signal 300, (ii) determines the identifier 310 therefrom, which includes verifying the authenticity of the identifier 310, to yield an authenticated identifier, and (iii) sends a processed signal, i.e., the authenticated identifier to the permissions module. I have depicted this process in the demonstrative below, identifying the disclosure from the specification corresponding to the steps of the process.



Demonstrative 5

87. As such, the specification fully supports the limitations recited in claim elements [10.b] and [10.e.2], i.e., “an identification receiver ... to provide the authenticated first identifier of the aerial system identifier signal to the permission module.”

88. Regarding the dependent claims, i.e., SCs 11-18, Petitioners have not presented any additional arguments other than their dependence on independent SC. These claims are also fully supported by the specification as PO described in the RMTA. *See* RMTA at 2-19.

IX. SCs 10-18 ARE PATENTABLE

A. SCs 10-18 Are Clear, Not Indefinite

1. Claim Element [10.d]

89. Regarding claim element [10.d], Petitioners essentially repeat the erroneous allegations and arguments made in arguing that claim element [10.d] lacks written description support. *See* Opp. at 3-4; EX1024 (Chowdhary Decl), ¶51. Specifically, Petitioners state that claim element [10.d] is “indefinite because it introduces a logical inconsistency that precludes a person of ordinary skill in the art from determining the claim’s scope with reasonable certainty.” *See* EX1024 ¶¶51-52 (alleging that the only source of the second identifier functioning as a second factor identifier, is the identifier transmission system).

90. These allegations and arguments are erroneous. In particular, the limitations recited in claim element [10.d] themselves are clear: “the identification receiver is configured to receive:” (i) “the first identifier from the [UAS], and (ii) a second identifier from a computing system that is remote relative to the discrimination system.” Thus, the claim language itself clearly defines the claim scope.

91. Moreover, as discussed above, the specification explicitly discloses three embodiments: (i) Embodiment A: receiving an aerial system identifier transmitted from the aerial system; (ii) Embodiment B: receiving an aerial system identifier transmitted from a remote computing system; and (iii) Embodiment C: receiving two aerial system identifiers that are both transmitted from the aerial system. *See supra* § VIII.A. This would have informed a POSITA of an embodiment where two aerial system identifiers are received – one from the aerial system and the other from a remote computing system, as disclosed in Embodiments A-C. *See id.* (Demonstrative 1-3) Accordingly, in light of the clear claim language and sufficient disclosure therefore in the specification, a POSITA would have understood the claim’s scope with reasonable certainty. As such, in my opinion, claim element [10.d] is not indefinite.

2. Claim Element [10.g]

92. For this claim element, Petitioners argue that the claims, specification, and prosecution history of the '199 Patent “do not provide any insight into the meaning of ‘preemptively enabled,’ making SC 10’s scope ambiguous and unclear.” Opp. at 4; EX1024 (Chowdhary Decl), ¶54. In my opinion, that argument is erroneous.

93. Petitioner’s allegation that a POSITA cannot sufficiently understand “preemptively enabled” is an error first because it ignores the commonly understood meaning of the word “preemptively,” which is “to seize upon to the exclusion of others.” EX2025. Preemption also means “to prevent from happening or taking place,” i.e., to “forestall” or to “preclude.” *Id.*

94. The '199 patent discloses a preemption process that is consistent with the commonly understood meaning of that term. The '199 patent’s system seizes upon the aggressive option of taking a disruptive action to the exclusion of other less aggressive options, such as communicating with the aerial system, allowing it to leave airspace, etc. *See supra* § VII.B. Thus, the less aggressive options are forestalled or precluded. This may prevent an unauthorized aerial vehicle from continuing its operation in a restricted airspace, which the aerial vehicle could have accomplished if one of the less aggressive options were chosen instead of preemptively enabling the disruption system.

95. As FIG. 5 depicts, and the discussion of “preemptively enabled” in the specification states, in certain more time-sensitive situations, a disruption system may be enabled without exercising the less aggressive options described above. For example, as soon as it is determined that a received identifier is not authenticated, the disruption system may be enabled, without ever allowing the UAV to leave the airspace voluntarily after communication occurs between the UAV’s pilot and the disruption system. *See* EX2002, 37:8-18; EX1001, 18:31-47. Moreover, if a UAV does not provide an identifier, and none is detected by the identification system, the disruption system may also be enabled without even contacting the pilot of the UAV. *See* EX2002, 37:8-18; EX1001, 19:31-47. It is the omission of such less aggressive options “if certain conditions are met” that causes the disruption system to be *preemptively* enabled. Thus, the specification both clearly describes and depicts clearly the “preemptively enabled” feature of the disruption system.

96. Petitioners also argue that the ’199 patent “does not differentiate between the meaning of ‘preemptively enabled’ and ‘enabled,’ which sows uncertainty into SC 10.” Opp. at 4 EX1024 (Chowdhary Decl), ¶54. In support of this argument, Petitioners allege that in FIG. 5, upon meeting any of the three conditions 500, 501, 502, the process “goes directly to being ‘[e]nable[d]’ at step 503.” EX1024 (Chowdhary Decl), ¶56. Based on FIG. 5, Petitioners allege that it

would be “unclear to persons of ordinary skill in the art [] whether the meaning of ‘preemptively enabled’ is the same or different to ‘enabled.’” Opp. at 5-6 (emphasis omitted); EX1024 (Chowdhary Decl), ¶56. Petitioners also allege falsely that during my deposition I equated “‘preemptively enabled’ to ‘activate.’” Opp. at 6; EX1024 (Chowdhary Decl), ¶57 (citing EX1023 at 80:2-15, 84:21-85:1).

97. Again, Petitioners’ allegation that a POSITA cannot sufficiently distinguish “enabled” from “preemptively enabled” is erroneous, because Petitioners ignore the well-understood meaning of “preemptive,” and the disclosure of the ’199 patent with reference to FIG. 5 that is discussed above. In light of the written description reciting “preemptively enabled” that is quoted above, *see* EX2002, 36:20-24, 37:8-18, and the process depicted in FIG. 5 itself, the meaning of “preemptively enabled” would have been clear to a POSITA. *See supra* § VII.B.

98. Thus the ’199 patent clearly delineates an enablement of a disruption system, e.g., based on a UAV being deemed not permitted, and after the exercise of one or more less aggressive option, and a preemptive enablement of the disruption system without exercising any of the less aggressive options.

99. A POSITA would further understand this general flow is short-circuited, i.e., the check for the condition 502 can be omitted, if condition 501 is met. A POSITA would have readily understood the omission of a step that is

otherwise performed in a different scenario as “preemptive.” In fact, the specification states so. EX2002, 36:20-24 (“preemptively enabled if certain conditions are met”). If condition 500 is met, the checks for both conditions 501, 502 are omitted – the steps that are otherwise performed in a different scenario. See EX1001, FIG. 5. A POSITA would have readily understood the omission of two steps that are otherwise performed in a different scenario also as “preemptive.”

100. Regarding my testimony, when asked to explain “preemptively enabled,” I stated that the disruption system of the ’199 patent is “preemptively enabled if certain conditions are met.” EX1023 at 80:5-15. When Petitioners’ Counsel asked about “activating the disruption system preemptively enabling the disruption system,” I responded by saying “[i]f certain conditions are met.” *Id.* 84:2-85:3. Thus, contrary to Petitioners’ allegation, I did not equate preemptively enabled to activate.

101. In summary, a POSITA would not have taken into account only the label “Enable disruption system” of the process step 503. Rather, a POSITA would have considered the figure as a whole, including the bypass paths depicted in the figure, and also the written description that discusses both the “enabled operation mode,” and “preemptively enabled.” In light of this disclosure, a POSITA would not have clearly understood the meaning “preemptively enabled” as recited in claim element [10.g].

102. Accordingly, a POSITA would not have found SC 10 indefinite.

X. SCs 10-18 ARE PATENTABLE – NOT OBVIOUS

A. Key Elements of Proposed Substitute Claim (SC) 10

103. The key elements of SC10 include:

10[.pre] “A discrimination system comprising:”

[10.a] “an identifier transmission system coupled to an unmanned aerial system” [UAS]

[10.d] “identification receiver is configured to receive ... a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system”

[10.e.1] “verify an authenticity of the first identifier using the second identifier.”

104. As I explain below, none of the grounds that Petitioners have asserted teach each and every one of the above-identified limitations of SC 10.

B. Grounds Based on Jarrell

105. The system of Jarrell and Whitmarsh is representative of Petitioner’s Jarrell-based invalidity grounds. In that system, a UAV provides a first identifier to a ground-based remote control center, then the ground-based remote control center
148 “provide[s] a list, and the communications station 101 may compare the UAV

registration or license identifier” provided by a UAV, to the *list* provided by the remote control center and “make a determination regarding the UAV’s compliance.” EX1024 (Chowdhary Decl) ¶¶68. More specifically, Petitioners allege that in a combination using Whitmarsh and Jarrell, Whitmarsh’s system, i.e., an “identification system” that receives a UAV MAC address can also receive “a *list* of valid MAC address identifiers,” like Jarrell’s *list*. *Id.* ¶¶80. Petitioners then allege that a “valid MAC address identifier” that is received in a list from a remote control center, and that corresponds to the MAC address identifier received from the UAV, is a “second identifier” functioning as a “second factor identifier.” *Id.* ¶¶80.

106. In my opinion, this argument is flawed for at least three reasons. First, Jarrell’s list of valid MAC identifiers is not a “second identifier.” A *list* of identifiers for various different aircraft is not itself an identifier because it does not serve to identify any particular aircraft. Indeed, the list of MAC identifiers in Jarrell is more analogous to the ’199 Patent’s “aerial system permissions 307” permissions module. EX1001, Fig. 1, Fig. 3 (element 307), 4:9-29, 17:12-18:55. Like the list of permissions 307 in the ’199 Patent’s permission module, Jarrell’s “list” of MAC addresses is simply an authoritative list for which an identifier can be checked against. But, like permissions list 307, Jarrell’s list of identifiers it is

not itself an identifier because it contains data about multiple different aircraft.

Because it is not specific to any aircraft, it is not an identifier.

107. Second, as I explained above, in the context of authentication, if one identifier is one factor, e.g., something you have,” the “second” factor must be something other than “something you have.” The second factor must either be “something you know” or “something you are.” *See supra* § VI. In the proposed combination, the first identifier is a MAC address, i.e., “something you have.” A matching identifier in Jarrell’s list of MAC identifier is not a different factor. In fact, it is not even a different instance of the “what you have” factor; it is the same identifier. Therefore, Jarrell does not teach a “second identifier functioning as a second factor identifier.”

108. Third, a specific identifier that is included in Jarrell’s list and that matches an identifier received from a UAV (i.e., the “first identifier” as claimed) is not “a second identifier” that can be used to “verify an authenticity of the first identifier,” as claim element [10.e.1] recites. This is because, if the second identifier is to be used to determine the authenticity of the first identifier, the two identifiers must be different but associated with the same entity, e.g., a UAV.

109. To illustrate, suppose a rogue UAV having a MAC identifier “X” steals the MAC identifier “B” of a UAV that is permitted to be in a restricted airspace, and transmits the identifier “B” as its own. A list in Jarrell’s system may

include the identifiers “A,” “B,” and “C.” Jarrell’s system would match the identifier “B” received from the UAV with the identifier “B” in the list, and would determine the rogue identifier as authentic. The identifier “B” was found in the list because it is the same as the received identifier “B,” and as such, the former does not and cannot verify the authenticity of the latter. The matching identifier found in the list tells us something about the permissions associated with identifier B, but it provides no protection whatsoever against “identifier reproduction” that the ’199 patent describes, such as that of identifier “B” by the rogue UAV.

110. In summary, in combinations using Jarrell, neither a received list nor a matching identifier therein meets at least the requirements of claim elements [10.d] and [10.e.1].

C. Grounds Based on Pasko

111. Regarding Pasko, Petitioners state that Pasko’s “computing platform authenticates the UAV by comparing the UAV serial number and government registration number of the UAV credentials against stored identification information and a government registration number of the account information.” EX1024 (Chowdhary Decl) ¶69. Pasko’s stored “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.* ¶76

(citing EX1026, ¶¶37-38). Petitioners then allege that the account information may be received from a remote computer, such as “Jarrell’s remote control center,” *id.* ¶77, and argues that Pasko’s “technique verifies an authenticity of the UAV (and its credentials) in multiple ways.” *Id.* ¶76.

112. This argument is incorrect. In general, Pasko may describe authenticating a UAV (though not reliably, as I discuss below), but does not teach authenticating a received *identifier* of a UAV. This distinction is of paramount importance. Pasko states:

UAV platform 230 may *compare the credentials* of UAV 220 with *UAV account information* stored in data storage 235 (e.g., information associated with authenticated and registered UAVs 220, such as identification numbers of UAVs 220, public and/or private keys of UAVs 220, account status information, etc.) in order to determine whether UAV 220 is authenticated for using UAV platform 230 and/or one or more of networks 240-260.

Id. ¶37.

113. To reiterate, Pasko *never* describes authenticating a received *identifier* of a UAV. Pasko describes using different identifiers in the received UAV credentials for different purposes. For example, “compar[ing] the serial number to the UAV account information in data storage 235 to determine whether UAV 220 is registered with UAV platform,” and “compar[ing] the government registration number to the UAV account information in data storage 235 to determine whether

UAV 220 is registered with a government agency to legally fly in [regulated] airspace.” *Id.* ¶¶37-38.

114. Pasko’s technique however, does not *verify* the authenticity of the UAV’s serial number (or the authenticity of any other identifier). As with Jarrell, *see supra* § X.B, if a rogue UAV were to present a *stolen* identifier (serial identifier and/or government registration number), that identifier may be found in one of the records stored in Pasko’s data storage,⁹ and the accessed account information would identify registration and flying permissions for the stolen identifier, just as it would if that same identifier were presented to the system by its rightful owner. As such, though Pasko’s computing platform can authenticate (though falsely) the UAV transmitting the stolen credentials as properly registered and/or permitted to fly in a restricted airspace, Pasko’s technique does not determine whether the “UAV credentials,” e.g., the serial number, the government registration number, themselves, are authentic, i.e., whether they actually belong to the UAV sending the credentials or whether they are stolen / spoofed. *See supra* ¶¶108-109, **Error! Reference source not found..**

115. Petitioners also allege that Pasko’s “technique verifies an authenticity of the UAV’s serial number as the serial number is associated with a UAV that is

⁹ The information in the data storage may be stored in “databases, tables, lists, trees, etc.” and may include the “UAV account information.” EX1026, ¶22.

properly registered with a government authority.” *Id.* Specifically, Petitioners contend that an identification receiver in Whitmarsh’s system “(1) receives credentials including the identifier UAV MAC address and government registration number from a UAV, ... and (2) 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.” EX1024 (Chowdhary Decl) ¶¶77, 80 (“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”).

116. There is a significant flaw in Petitioners’ allegations and contentions. The scenario alluded to above is an outcome that Petitioners have contemplated. It is not a process that Pasko discloses. Pasko itself (and none of the other references in the combination) discloses such a cross-checking of two identifiers that Petitioners contemplate.

117. In Pasko’s system, in order to *authenticate* one identifier using another identifier, a number of pre-conditions would have to be met and a number of steps would have to be followed, that neither Pasko nor Petitioners mention. First, the credentials sent by the UAV and received at the computing platform must include at least two identifiers, e.g., a serial number and a government registration

number. *See* EX1026, ¶37. Then, the UAV account information stored in the data storage must also include corresponding instances of each of those two identifiers, that can then be used for the respective verification of the two identifiers included in the credentials received by the computing platform. Then, a mismatch as discussed below, can be used to determine if any of the identifiers in the received credentials is fake/unauthentic.

118. As an illustrative example, suppose a rogue UAV sends a fake / stolen serial number S1 and a fake, stolen government registration number G9. When the stored account information corresponding to serial number S1 is retrieved, that account information may include a government registration number G1 that corresponds to the authentic UAV actually having the serial number S1. The platform must then determine that G1 in the account information does not match G9, and thus determine that S1, G9, or both are not authentic. Pasko does not teach such cross-checking. Petitioners have not explained why a POSITA would undertake such a modification.

119. To summarize, to authenticate one identifier using another identifier in Pasko's system, *at least* the following basic steps would have to be taken:

- i. the credentials transmitted by the UAV, as admitted by Petitioner, include two identifiers— UAV serial number and government registration number of the UAV ;

- ii. the account information retrieved using any one of the two identifiers included in the UAV credentials must include two identifiers corresponding, respectively, to the two identifiers included in the UAV credentials mentioned in (i); and
- iii. functionality must be provided to check that each of the two identifiers in the UAV credentials matches the corresponding identifier in the retrieved account information.

120. Pasko is entirely silent on any such cross-verification and authentication steps for the two identifiers mentioned by Petitioner, whether using the serial numbers, the government registration numbers. Even Petitioners have not described the pre-requisite conditions and steps that I have detailed above.

121. Additionally, *none* of UAV's serial number, government registration number, and any of the keys that Pasko describes, is a "*second factor* identifier." This is because, each of these identifiers (to the extent a key can be considered an identifier), belongs to the category "what you have." None of these entities is "something you know" or "something you are." As such, none of these entities can function as a "second factor identifier" with respect to any of the entities. *See supra* § VI.

122. Therefore, the proposed combination of Pasko and Jarrell does not meet the limitations of claim element [10.d].

123. Accordingly, combinations using Jarrell or Jarrell and Pasko do not teach or suggest at least [10.d] and [10.e.1].

D. Grounds Based on Viggiano and Gong637

124. For claim element [10.d], for the combinations that rely on Viggiano and Gong637, Petitioners state that Viggiano discloses “a message authentication code 38 formed from identification information 22 of the aircraft transmitter (which identifies the aircraft) and a secret key 36 of the aircraft.” EX1024 (Chowdhary Decl) ¶¶92; EX1007 ¶¶0004, 0006-0007, 0011-0028, FIGS. 1-3. Petitioners also states that “Gong637 discloses a UAV that 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.” Opp. at 20; EX1024 (Chowdhary Decl) ¶¶93; EX1022, ¶¶0087-0098.

125. Based on the observations noted above, Petitioners allege that Whitmarsh’s identification receiver can receive a MAC ID from the UAV, where the MAC ID is the claimed “first identifier,” and also receive “a message authentication code formed from identification information of the UAV ... from a second communication unit of the UAV.” Opp. at 21-22; EX1024 (Chowdhary

Decl) ¶94. Petitioners then allege that the message authentication code is the “second factor identifier” and that “second communication unit of the UAV” of the proposed combination is “a computing system that is remote relative to the discrimination system.” Opp. at 22-23; EX1024, ¶94.

126. This argument is wrong because in the proposed combination, the second communication unit of the UAV would transmit the message authentication code, and is therefore at least a part of “an identifier transmission system coupled to” the UAV. Per the preamble of claim 10 and claim element [10.a], however, the “identifier transmission system” is part of the discrimination system. As such, the second communication unit of the UAV is a part of and not “remote relative to” the discrimination system.

127. Additionally, the message authentication code 38 is generated from Whitmarsh’s MAC ID. The message authentication code 38 and the MAC ID are both “something you have.” As such, neither of these can function as a “second factor identifier” with respect to the other. *See supra* § VI.

128. Accordingly, Viggiano in combination with Gong637 does not teach or suggest at least 10[.pre], [10.a], and [10.d].

E. Petitioners’ Asserted Grounds

129. Petitioners have asserted 12 grounds, Grounds 7B through 10B (based on Jarrell), Grounds 7C through 10C (based on Jarrell and Pasko), and Grounds

11-14 (based on Viggiano and Gong637). These Grounds rely only on Jarrell, Pasko, or Viggiano in view of Gong637 re.: claim the preamble 10[.pre] and claim elements [10.a], [10.b], [10.d], and/or [10.e.1]. Therefore, each of these Grounds fails, because Jarrell, Pasko, Viggiano, and Gong637, in combination as Petitioner proposes, do not teach or suggest the limitations of claim the preamble 10[.pre] and claim elements [10.a], [10.b], [10.d], and/or [10.e.1].

XI. CONCLUSION

130. For the foregoing reasons, it is my opinion that the proposed substitute claims 10-18 are patentable.

131. I currently hold the opinions that I have expressed in this declaration. My analysis may continue, however, as I may acquire or receive additional information or insights that may result in revised or supplemental observations or opinions.

132. I understand this declaration may be used as evidence in the instant IPR proceeding before the PTAB.

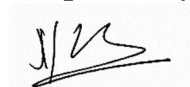
133. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,

under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the '199 patent.

134. I declare under penalty of perjury that the foregoing is true and correct.

Dated: June 22, 2026

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'N. Papanikolopoulos', written on a light gray rectangular background.

Dr. Nikolaos Papanikolopoulos

Appendix A: Authentication and Foundation for Cited Exhibits

135. Exhibit EX2008 is a document published by the U.S. Department of Commerce. It bears the seal of the U.S. Department of Commerce, and the signatures of the Acting Secretary of the Department of Commerce, and of the Under Secretary of Commerce for Standards and Technology and Director. I downloaded the document identified as EX2008 on June 15, 2026. Based on my review of the appearance of this document and its contents, I believe that this document is what it purports to be and I am informed by Counsel and understand that this document is self-authenticating under F.R.E. 902(1).