

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Axon Enterprise, Inc., Dedrone Holdings, Inc., and Skydio, Inc.

Petitioners,

v.

Airspace Defense, Inc.

Patent Owner

Case No. IPR2025-00530

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

**PATENT OWNER REPLY TO OPPOSITION
TO REVISED MOTION TO AMEND**

TABLE OF CONTENTS

I.	PO HAS MET ITS BURDEN FOR ALL PROPOSED SUBSTITUTE CLAIMS.....	1
A.	<i>The specification describes limitation 10.d.....</i>	<i>1</i>
B.	<i>The specification describes limitation 10.e2.....</i>	<i>2</i>
II.	SCs 10-18 ARE NOT INDEFINITE	4
A.	<i>A POSITA Would Readily Understand Limitation [10.d]</i>	<i>4</i>
B.	<i>A POSITA Would Readily Understand Limitation [10.g]</i>	<i>4</i>
III.	SCs 10-18 ARE PATENTABLE OVER ALL CITED COMBINATIONS.....	6
A.	<i>Petitioners' Grounds Based on Jarrell Fail to Show Obviousness</i>	<i>6</i>
B.	<i>Petitioners' Grounds Based on Pasko Fail to Show Obviousness</i>	<i>8</i>
C.	<i>Petitioners' Grounds Based on Viggiano and Gong637 Fail to Show Obviousness.....</i>	<i>11</i>

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: The Italian Association for Information Systems</i> . Heidelberg:

Exhibit No.	Description
	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
EX2017	A library catalog MARC record for <i>Information Systems</i> :

Exhibit No.	Description
	<i>Crossroads for Organization, Management, Accounting and Engineering: ItAIS: The Italian Association for Information Systems, 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</i>
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.", <i>available at https://web.archive.org/web/20200113202746/http://www0.cs.ucl.ac.uk/staff/F.Sarro/resource/papers/B2%20e%20C11_CameraReady.pdf</i>.
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, Naval Postgraduate School Monterey (2004), <i>available at</i>

Exhibit No.	Description
	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> , available at https://archive.org/details/wirelessnetworks109451246/page/n1/mode/2up
EX2023	A library catalog MARC record for <i>Lecture Notes in Computer Science</i> , available from Penn State University Library at 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), as sourced from the Penn State University Library's collection.
EX2025	Merriam-Webster Dictionary, Definition of "preempt," as obtained from https://web.archive.org/web/20150911233241http://www.merriam-webster.com/dictionary/preempt

I. PO HAS MET ITS BURDEN FOR ALL PROPOSED SUBSTITUTE CLAIMS

A. The specification describes limitation 10.d

Petitioners argue that the specification fails to disclose a second identifier originating from somewhere other than the identifier transmission system. Opp., 1.

However, the specification 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. “[T]he aerial system identifier 310 is preferably dynamic” but can be static. EX2002, 14:16-17. Moreover, the “dynamic aerial system identifier can be generated on-board the aerial system 100, [or] generated *remotely* [] e.g., at a *remote computing system*.” *Id.*, 14:16-15:2. “[A]erial system identifier signal 300” is received by “the identification receiver 102.” *Id.*, 14:6-8.

“[T]he 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.” *Id.*, 4:15-22. And, it states that “the preferred embodiments include every combination and permutation of [the] various system components.” *Id.*, 39:6-9. Reading these disclosures in context with each other demonstrates that one or two identifiers may be used, and either may be remote or local to the UAV. EX2005, ¶¶72-79.

Petitioners also argue that “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. To the contrary, 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. And, the specification discloses that the “identification receiver 102, [] functions to receive the aerial system identifier signal 300.” *Id.*, 4:57-59. These passages disclose that the remote computing system—outside of the discrimination system—can generate and transmit identifiers and that such identifiers are received by the identification receiver. Thus, Petitioners’ argument appears to rely on improperly rewriting the claim to require that the second identifier must be received *directly* from the remote computing system. However, the claim is not so limited. Rather, in context of the specification, a POSITA would understand the claim to encompass second 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). The disclosure of the indirect species is adequate disclosure for the genus limitation, as it is representative of the full scope of the claim. EX2005, ¶¶80-82; *see Hologic, Inc. v. Smith & Nephew, Inc.*, 884 F. 3d 1357, 1362 (Fed. Cir. 2018).

B. The specification describes limitation 10.e2

Petitioners argue that limitation 10.e2’s “provide the authenticated first identifier

... to the permission module” is not described, asserting that “raw or processed” signals, decrypted signals, and verification of identifier 310 fail to disclose providing an authenticated first identifier to a permission module. Opp. at 3.

To the contrary, 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, chipset 608 can determine the aerial system identifier 310 from a received identification signal 300. EX2005, ¶¶83-84. The specification also 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, chipset 608 can verify identifier 310’s authenticity, yielding an *authenticated* identifier. EX2005, ¶85.

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; *see also id.*, Fig. 1 (showing “aerial system identifier / ID” input to permissions module 103). Thus, a POSITA would understand that the processed signal 300 sent to the permissions module includes the identifier 310, which has been authenticated. EX2005, ¶¶85-88.

II. SCS 10-18 ARE NOT INDEFINITE

A. A POSITA Would Readily Understand Limitation [10.d]

Petitioners argue that limitation [10.d] is indefinite because it recites a “discrimination system that includes an identifier transmission system” and asserts that “the only source of the second identifier functioning as a second factor identifier is the identifier transmission system.” Opp. at 3-4. Petitioners incorporate by reference their written description arguments for limitation 10.d, arguing that the “identifier transmission system ... cannot logically be remote relative to” itself. *Id.* That argument fails for largely the same reasons discussed above with respect to written description. *Supra* I.A. In particular, Petitioners misread the claim and specification in concluding that “the only source of the second identifier functioning as a second factor identifier is the identifier transmission system.” EX2005, ¶¶89-91. As noted, the claim is consistent with the specification, which provides that identifiers can originate from a remote computer system.

B. A POSITA Would Readily Understand Limitation [10.g]

Petitioners argue that limitation [10.g] is indefinite, asserting that the term “preemptively enabled” lacks reasonable certainty. Opp. at 4-5. But those are ordinary words of the English language, and Petitioners ignore their ordinary meaning. In particular, “preemptively” conveys “to seize upon to the exclusion of others” or “to prevent from happening or taking place,” i.e., to “forestall” or to “preclude.” EX2005, ¶¶92-93; EX2025. This is consistent with the specification

which discloses, in certain scenarios, aggressively taking a disruptive action to the exclusion of other less aggressive options, forestalling or precluding the less aggressive options. EX2005, ¶94. In particular, as shown in Fig. 5 and described on pages 36-37 of the application, there are time sensitive situations where, as soon as it is determined that a received identifier is not authenticated or not provided, the disruption system may be preemptively enabled. *Id.* ¶95; EX. 2002, 36:20-38:18. This forestalls and precludes the less aggressive options, such as “contacting the aerial system pilot prior to disruption system activation” to allow the UAV to leave the airspace voluntarily. *Id.*

Petitioners also assert that the difference between “enabled” and “preemptively enabled” is unclear. But, as discussed, the plain and ordinary meaning of “preemptive” and the disclosures of the specification, clearly delineates a non-preemptive 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 (e.g., without exercising the less aggressive options). EX2005, ¶¶93-94. In particular, in the context of Figure 5, a POSITA would understand from the dotted lines that the general flow can be short-circuited such that the disruption system is preemptively enabled, i.e., the check for the condition 502 can be omitted, if condition 501 is met. EX2005, ¶¶95-98; *see also* EX2002, 36:20-24 (“preemptively enabled if certain conditions are met”). If

condition 500 in Figure 5 is met for example, the checks for both conditions 501, 502 can be omitted – forestalling and precluding the steps that are otherwise performed in different scenarios and thus preemptively enabling the disruption system. EX2005, ¶¶99-102.

III. SCS 10-18 ARE PATENTABLE OVER ALL CITED COMBINATIONS

Petitioners present obviousness grounds 7B through 14 (Opp. at 6), but these can be generally grouped into (i) grounds based on Jarrell (Opp. at 7-9), (ii) grounds based on Pasko (Opp. at 9-12); and (iii) grounds based on Viggiano and Gong637 (Opp. at 19-25).

A. Petitioners’ Grounds Based on Jarrell Fail to Show Obviousness

Petitioners assert that Jarrell discloses a “control center 148’ that “provide[s] a list, and the communications station 101 may compare the UAV registration or license identifier to the list and make a determination regarding the UAV’s compliance.”” Opp. at 8. They allege that Jarrell’s “list of valid MAC address identifiers that includes a valid MAC address identifier relevant to the UAV” is the “second identifier,” and that the UAV’s MAC address is a first identifier. Opp. at 13-14, 16-17. They argue that the MAC address list is a “second factor” “because it is a second identifier to the UAV’s transmitted MAC address and authenticates the transmitted MAC address and determines whether the UAV is compliant.” *Id.*

Petitioners’ Jarrell-based theories fail for several reasons. Firstly, Jarrell’s “list

of valid MAC identifiers” does not satisfy limitation [10.e1] because a *list* of identifiers for various different aircrafts is not itself an identifier—it does not serve to identify any particular aircraft. EX2005, ¶¶105-106. Rather, Jarrell’s list of MAC identifiers is analogous to the “aerial system permissions 307” permissions module of the ’199 Patent. *Id.*; EX1001, Fig. 1, Fig. 3 (element 307), 4:9-29, 17:12-18:55. That is, it is an authoritative list for which an identifier can be checked against, but it is not an identifier because it is not specific to any one aircraft.

Second, Jarrell’s list is not a “second factor.” The meaning of second factor authentication is known in the art. EX2005, ¶¶46-52.¹ The relevant factors are “something you know,” “something you have,” or “something you are.” *Id.* Thus if the first factor is “something you have,” the “second” factor must be something other than “something you have” (i.e. “something you know” or “something you are.”). In the proposed combinations using Jarrell, the first identifier is a MAC address, i.e., “something you have.” EX2005, ¶107. Thus, a matching MAC address in Jarrell’s list is not a different factor. It is not even a different instance of the “what you have” factor; it is the same identifier. *Id.* Therefore, Jarrell does not disclose or suggest a “second identifier functioning as a *second factor* identifier.” Moreover, Petitioners and their expert’s analysis is inadequate because they fail to discuss or address the

¹ The declaration of June Munford demonstrates that the new reply exhibits are authentic and were publicly available as of their identified dates. EX2006.

well-known “something you know,” “something you have,” or “something you are” factors associated with second factor authentication.

Third, the specific identifier in Jarrell’s MAC address list 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.” 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. EX2005, ¶108. That is, Jarrell’s identifier does nothing to address a maliciously spoofed, cloned, or tampered identifier; it only provides the permissions associated with a particular identifier, not whether that identifier is *authentic*. EX2005, ¶¶109-110; *see also* ’199 Patent at 2:62-64 (a “second factor identifier” acts as a “secondary authenticator for the aerial system to prevent tampering and/or identifier reproduction.”).

B. Petitioners’ Grounds Based on Pasko Fail to Show Obviousness

Petitioners assert that Pasko discloses “a UAV transmits ‘credentials,’ that include an ‘identification number,’ ‘serial number,’ and ‘government registration number’—all associated with the UAV—to a computing platform 230” Opp. at 10. Petitioners allege that Pasko’s “received account information” is the “second identifier,” and that the MAC address or government registration number of the UAV would be the first identifier. Opp. at 14-15, 17. They argue that the account information is a

“second factor” “because it is a second identifier ... to the UAV’s transmitted MAC address that authenticates the MAC address.” Opp. at 15. Petitioners also argue that the “account information” is a “second identifier” because it is “a different piece of information (e.g., a government registration number) from the UAV MAC address that is used in an additional comparison (e.g., using government registration numbers), which further provides the account information.” Opp. at 14.

Petitioners’ Pasko-based theories fail for several reasons. First, although Pasko generally describes authenticating a UAV, it does not authenticate a received *identifier* of a UAV, as recited in limitation 10.e1. Rather, Pasko’s UAV platform *compares the credentials* of a UAV *with UAV account information* stored “in order to determine whether UAV 220 is authenticated for using UAV platform 230.” EX1026, ¶ 37; EX2005, ¶¶111-112. For example, Pasko “compar[es] the serial number to the UAV account information ... to determine whether UAV 220 is registered with UAV platform” and “compar[es] 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.” EX1026, ¶¶ 37-38. But none of these disclosures relate to authenticating an identifier—Pasko’s account information does nothing to address a maliciously cloned or tampered identifier. EX2005, ¶¶ 113-114; *see also* ’199 Patent at 2:62-64. In short, verifying that a UAV’s identifier is registered to fly does not verify whether the identifier a UAV

provides is authentic.

Additionally, Pasko's "account information" does not constitute a "second factor" for essentially the same reasons discussed above with respect to Jarrell. *Supra* III.A. In particular, Petitioners fail to analyze the "something you have," something you know," or "something you are" factors. Indeed, the account information for the UAV is "something you have," as are its serial number and government registration number. EX2005, ¶ 121. Thus, the "account information" is not a "second factor."

Petitioners also present an additional theory with respect to Pasko, asserting that the combination "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." Opp. at 11. But that is not a disclosure rooted in Pasko or any of the other references, nor do Petitioners articulate a motivation to modify the references to implement this functionality. In particular, neither Pasko itself nor any of the other references discloses cross-checking of two identifiers that Petitioners assert. EX2005, ¶116. To cross-check two identifiers, it would require that the UAV sends two identifiers to the computing platform and that the stored account information contains those same two identifiers stored such that they are associated with each other, and it would require that the computing platform is specifically configured to cross-check those identifiers. EX2005, ¶¶117-120. But

Pasko does not teach these steps. Instead, as discussed, it discloses generically “comparing” the credentials from the drone with the account information, not cross-checking one credential against the other. EX1026, ¶¶10, 20, 22, 26, 35-42. And Petitioners’ motivation to combine theory articulates no reasoning for a motivation to modify the references in that manner. Opp. at 9-12; EX1024 ¶77.

C. Petitioners’ Grounds Based on Viggiano and Gong637 Fail to Show Obviousness

In Petitioners’ grounds based on Viggiano and Gong637, Petitioners argue that the UAV’s MAC address is the first identifier and that Viggiano’s “message authentication code (AC)” —is a second identifier and second factor because it is “formed from identification information and a unique secret key of the UAV” Op. at 19-20, 22-23. However, this theory fails for at least two reasons.

First, Petitioners’ Viggiano-Gong637 theory fails to satisfy the requirement that the second identifier come from “a computing system that is remote relative to the discrimination system.” In particular, in Viggiano, the message AC is generated by the aircraft and transmitted through its “ADS-B transmitting system.” EX1007, ¶12 (“each aircraft is broadcasting its ID 22 and specific data 24”), ¶13 (“The MAC 38, the ADS-B transmitter's ID 22 and the ADS-B transmitter's specific data 24 are then transmitted to the Authenticator 10 in an authentication response 18”). Similarly, in Gong637, the “identification” comes from the UAV. EX1022, ¶¶0094, 0122. Because the “identifier transmission system coupled to an unmanned aerial system”

is a component of the claimed “discrimination system,” an identifier originating from the UAV is not “remote relative to the discrimination system.” Relying on Gong637 as having a UAV with two communication systems, Petitioners assert that the combination would use one communication system to send the “first identifier” and the second communication system to send the alleged second identifier (Viggiano’s message AC). EX1024 ¶¶93-94. But in that scenario, the second communication system would still be part of “an identifier transmission system coupled” to the UAV as it would be transmitting the alleged second identifier. EX2005, ¶¶124-125. Because the “identifier transmission system” is part of the discrimination system, the UAV’s “second communication system” in the proposed combination would not be “remote” to the discrimination system. *Id.*, ¶ 126.

Second, Petitioners’ Viggiano-Gong637 theory fails because it fails to disclose or suggest “the second identifier functioning as a second factor identifier.” Like its theories based on Jarrell and Pasko, Petitioners and their expert do not analyze the factors relevant to whether something is a “second factor” (i.e. “something you know,” “something you have,” or “something you are.”). Moreover, Petitioners’ theory is that the first identifier is the drone’s MAC ID and the second identifier is a message authentication code generated from that same MAC ID. Opp. at 23. But both simply use the MAC ID, and are thus “something you have.” EX2005, ¶126.

Respectfully submitted,

Dated: June 22, 2026

/ Suhrid Wadekar /

Suhrid Wadekar, Ph.D., Esq.
Registration No. 65,595
Counsel for Patent Owner
Airspace Defense, Inc.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I hereby certify that about June 22, 2026, a copy of the foregoing Patent Owner's Reply to Petitioners' Opposition to Patent Owner's Revised Motion to Amend, and its exhibits, are being served electronically (per counsel's consent) to lead and backup counsel of record for Petitioners as follows:

DLAxonDedroneIPRs@bakerbotts.com

chad.walters@bakerbotts.com

harrison.rich@bakerbotts.com

ellyar.barazesh@bakerbotts.com

nmatich@mckoolsmith.com

cleone@mckoolsmith.com

/ Suhrid Wadekar /

Suhrid Wadekar (Reg. No. 65,595)

PRINCE LOBEL TYE LLP

One International Place, Suite 3700

Boston, MA 02110

Tel: (617) 456-8000

Email: swadekar@princelobel.com