

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 Systems, Inc.

Patent Owner

Case No. IPR2025-00525

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

PATENT OWNER PRELIMINARY RESPONSE

Table of Contents

I.	INTRODUCTION.....	1
II.	THE '959 PATENT	1
A.	<i>Administrative Overview</i>	<i>1</i>
B.	<i>Prosecution History.....</i>	<i>2</i>
C.	<i>Subject Matter.....</i>	<i>2</i>
III.	CLAIM CONSTRUCTION.....	5
IV.	CLAIM 21 IS ENTITLED TO EARLIEST PRIORITY DATE OF JUNE 12, 2015	15
A.	<i>Claim 21 Is Entitled to Claim Priority to the '153 Provisional.....</i>	<i>15</i>
B.	<i>The '959 Patent Is Entitled to Claim Priority to the '071 PCT Application and to the '153 Provisional</i>	<i>17</i>
1.	The '959 Patent's Priority Chain is Not Broken and Meets the "Specific Reference" Requirement of 35 U.S.C. § 120	17
2.	Claim 21 Is Entitled to Claim Priority to the '071 PCT Application	25
V.	EACH OF GROUNDS 1-4 FAILS TO DEMONSTRATE UNPATENTABILITY OF CLAIM 21 BY A PREPONDERANCE OF THE EVIDENCE	32
A.	<i>Ground 1</i>	<i>32</i>
B.	<i>Ground 2.....</i>	<i>36</i>
1.	A POSITA Would Not Combine Taveira, Wang, and Gong.....	36
2.	The Taveira-Wang-Gong Combination Does Not Teach or Suggest "a Secure Identifier" Recited in Claim 21	43
C.	<i>Ground 3.....</i>	<i>49</i>
1.	A POSITA Would Not Combine Taveira, Qi, and Gong	49
2.	The Taveira-Qi-Gong Combination Does Not Teach or Suggest "a Secure Identifier" Recited in Claim 21	54
D.	<i>Ground 4.....</i>	<i>56</i>
1.	A POSITA Would Not Combine Gong and Wang-II	56

2. The Gong-Wang-II Combination Does Not Teach or Suggest a
“Secure Identifier” 57

VI. CONCLUSION 59

Patent Owner’s Exhibit List

Exhibit No.	Description
EX2001	PCT Request, International (PCT) Application No. PCT/US16/37071, filed on June 10, 2016
EX2002	PDF Copies of MPEP Editions and Revisions 1948 – 2023, https://www.uspto.gov/web/offices/pac/mpep/old/index.htm .
EX2003	Chapter 200 Types, Cross-Noting, and Status of Application, Manual of Patent Examining Procedure (MPEP) (1994)
EX2004	Chapter 200 Types and Status of Application; Benefit and Priority Claims, Manual of Patent Examining Procedure (MPEP) (2018)
EX2005	J. Ablon (Airmap), “Remote Identification,” https://www.icao.int/Meetings/UAS2017/-Documents/Jared%20Ablon_Stream%20A.pdf .
EX2006	Recommendation ITU-T X.509 (2016)
EX2007	P. Syverson, “A Taxonomy of Replay Attacks [cryptographic protocols],” Proceedings of the Computer Security Foundations Workshop VII, pp. 187-191 (1994), doi: 10.1109/CSFW.1994.315935.
EX2008	A.M. Espinoza, W.J. Tolley, and J.R. Crandall, “Alice and Bob, Who the FOCI Are They?: Analysis of End-to-End Encryption in the LINE Messaging Application,” 7th USENIX Workshop on Free and Open Communications on the Internet (FOCI 17) (2017), https://www.usenix.org/system/files/conference/foci17/foci17-paper-espinoza.pdf .

Exhibit No.	Description
EX2009	M.A. Harris and K. Patten, “Mobile Device Security Considerations for Small-and Medium-Sized Enterprise Business Mobility,” INFORMATION MANAGEMENT & COMPUTER SECURITY 22(1) 97-114 (2014), https://www.researchgate.net/profile/Mark-Harris-10/publication/263245514_Mobile_device_security_considerations_for_small-_and_medium-sized_enterprise_business_mobility/links/-5697cc4108ae1c427905200b/Mobile-device-security-considerations-for-small-and-medium-sized-enterprise-business-mobility.pdf.
EX2010	M. Cunche, M.A. Kaafar, and R. Boreli, “I Know Who You Will Meet this Evening! Linking Wireless Devices using Wi-Fi Probe Requests,” IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) (2012).
EX2011	J. Lindqvist et al., “Privacy-Preserving 802.11 Access-Point Discovery,” Microsoft Research Technical Report, MSR-TR-2009-7 at (2009), https://aaltodoc.aalto.fi/server/api/core/bitstreams/-7c421d1b-9ecd-45ee-8481-52f24ca272e5/content.
EX2012	M. Cunche, “I Know Your MAC Address: Targeted Tracking of Individual Using Wi-Fi,” 10 J. COMPUT. VIROL. HACK TECH. 219–227 (2014), https://doi.org/10.1007/s11416-013-0196-1.

Exhibit No.	Description
EX2013	W.S. Bhaya and S.A. AlAsady, "Prevention of Spoofing Attacks in the Infrastructure Wireless Networks," J. COMPUTER SCIENCE, 8(10) 1769-1779 (2012), https://web.archive.org/web/20150621205916id_-http://novintarjome.com/wp-content/uploads/2014/10/Prevention-of-Spoofing-Attacks.pdf.

I. INTRODUCTION

Petitioner has challenged Claim 21 of U.S. Patent No. 10,713,959 (the “’959 Patent”) on four Grounds. Grounds 1-4 fail principally because in each Ground, Petitioners have misinterpreted the claim limitation “secure identifier,” in alleging erroneously that an encrypted identifier is a “secure identifier.” As discussed below, encryption is neither necessary nor sufficient to provide the claimed “secured identifier.” Ground 2 fails for an additional reason that its proposed combination would be inoperable. Ground 3 and Ground 4 each fail for an additional reason that their alleged “secure identifiers” do not identify a connection, as required when properly construing Claim 21. Thus, Petitioners have not shown a reasonable likelihood of showing patentability of the only challenged Claim, Claim 21, and hence, it is respectfully submitted that the Petition be denied.

II. THE ’959 PATENT

A. Administrative Overview

The ’959 Patent issued from U.S. Patent Application No. 16/215,406 (the ’406 Application”), that was filed on December 10, 2018. EX1001, face page. The ’406 Application is a continuation of U.S. Patent Application No. 15/839,661 (the ’661 Application), filed on December 12, 2017, which is stated as a “continuation of” International Patent Application No. PCT/US2016/037071 (the ’071 PCT Application), filed on June 10, 2016. The ’071 PCT Application claims

priority to U.S. Provisional Patent Application No. 62/175,153 (the '153 Provisional), filed on June 12, 2015. The '661 Application also claims priority to U.S. Provisional Patent Application No. 62/566,450, filed on October 1, 2017. *See* EX1001, 1:7-22.

B. Prosecution History

During the prosecution of the '406 Application, the first Non-Final Office Action issued on August 7, 2019. EX1002 at 111. In that Office Action all pending claims (Claims 1-20)¹ were rejected on the ground of non-statutory double patenting based on Claims 1-20 of U.S. Patent No. 10,192,451. *Id.* at 113-114. In response to the filing of a terminal disclaimer by the Applicant, the pending claims were allowed. *See id.* at 61-68, 98-99.

C. Subject Matter

The '959 Patent discloses and claims a “a low altitude aircraft identification system,” as a response to the risk of damage or injury caused by such unregulated systems. EX1001, Abstract, 17:17-18:17, 1:35-2:3 (describing that due to the proliferating use of unmanned aerial vehicles (UAVs), there is an increased risk of “damage and/or injury due to the[] altitude, speed and weight” of the UAVs, “there

¹ A numbering error in the allowed Claims was corrected during issuance. As such, the allowed Claim 20 issued as Claim 21. *See* EX1002 at 48, 107 (Claim 18).

is [a] need to manage ... UAVs,” and that “an identification solution is needed”).

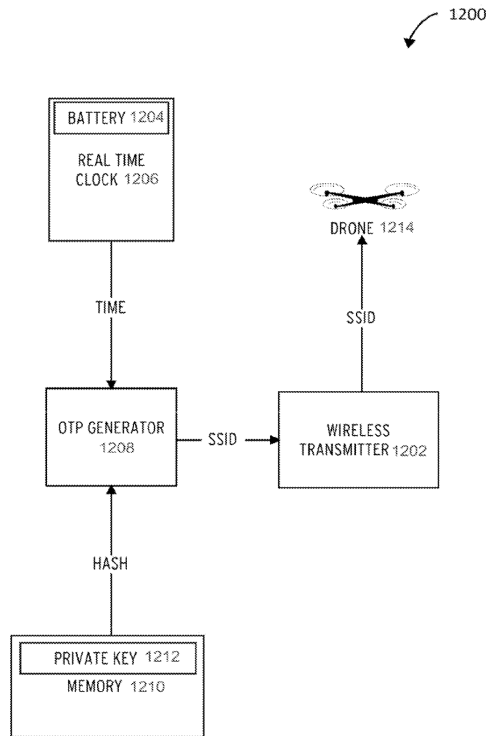
The '959 Patent describes that the conventional techniques for identifying and managing road vehicles and large aircraft are not suitable for UAVs for various reasons. *See id.*, 1:45-55. The '959 Patent further states that an identification solution that “allow[s] detection [of a UAV] in an automated manner using a device” is needed. *See id.*, 1:66-2:3.

The automated detection techniques that the '959 Patent describes can be classified as light-based techniques or radio frequency based (RF)-based techniques. *See generally, id.* The only challenged Claim, Claim 21, is directed to a device that uses RF-based technique for communicating information about a UAV, including its identification, to a UAV detection system. *See id.* 17:17-18:17.

Importantly, the '959 Patent claims that the radio communications module of the device uses a “*secure identifier*.” A secure identifier, as shown below, provides a **secure connection** for exchanging information (including the UAV’s identification information) between the UAV and a UAV detection system. The ‘959 patent describes this feature as a pre-requisite for facilitating safe, managed UAV operations. *See id.* 10:20-12:61 (recognizing that “there must be two-way trust between the server and the drone” and that without the trust “the risk of [unauthorized] transmission and reception is high,” and disclosing a system in

which trust between a UAV and a detection system is established through a “secured wireless communication”).

The '959 Patent describes that such a secure connection between a UAV and detection system can be established using predictably changing identifiers. *See id.* 11:17-24 (disclosing “frequently changing [] SSID [where] the probability of it being discovered and exploited or spoofed [is] greatly reduced”), 11:25-28 (“the transmission of the [wireless connection] identification must be reliable and unique, but also predictable to known parties so that the identification can be tracked ... to ensure that the wireless beacon was not changed or cloned”). To this end, the '959 Patent discloses several example systems featuring such predictably changing identifiers, including systems that employ rotating service set identifiers SSIDs, one-time-password (OTP) based SSIDs, timestamp and hash based identifiers, encrypted SSIDs that are timestamp based, and identifiers that are based on the expected UAV location at a given point in time. *See id.*, 6:63-7:30, 11:17-12:62, FIGS. 6, 9-13.



Id., FIG. 12.

In summary, the '959 patent teaches and claims the use of “secure identifiers” to deliver a critical pre-requisite for facilitating safe UAV operation: two-way trusted communication between a UAV and a UAV detection system where the communication is “not changed or cloned, etc.” *See id.*, 10:20-41; 11:25-29.

III. CLAIM CONSTRUCTION

Claim 21 recites a “radio communication module [that] is configured to utilize a **secure identifier**.” '959 Patent, 18:9-10. Petitioner states that it does “not present any constructions.” Pet. at 21-22. But, in alleging that “Claim 21 is not entitled to claim priority to the '153 Provisional” and to the '071 PCT

Application, Petitioner states that the “153 Provisional does not provide adequate written description for “secure identifier.” See Pet. at 7-9, 14-16. Patent Owner (“PO”) shows below, that based on a proper interpretation of “secure identifier,” the allegations above are incorrect. Thus, the parties dispute the interpretation of the claim term “secure identifier,” and it must therefore be construed. See *Vivid Technologies, Inc. v. American Science*, 200 F.3d 795, 803 (Fed. Cir. 2000) (“It is routine case management to require litigants to identify the aspects of their case that are material to the dispute” and “claim construction is for ‘resolution of disputed meanings’”) (quoting *U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997)).

“[C]laims are viewed and understood in the context of the specification and the prosecution history.” *Nature Simulation Systems Inc. v. Autodesk, Inc.*, 50 F.4th 1358, 1363 (Fed. Cir. 2022). “[C]laims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty.” *Id.* (quoting *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014)). Moreover, “the claim language as a whole supports” and thus informs, “the meaning given to the term.” *Hockerson-Halberstadt, Inc. v. Converse Inc.*, 183 F.3d 1369, 1375 (Fed. Cir. 1999); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (*en banc*) (“[T]he context in which a term is used in the asserted claim can be highly instructive.”).

Claim 21 recites, in relevant parts, “a radio communication module coupled to [a] radio frequency communication antenna” that is “coupled to [a] low-altitude aircraft.” EX1001 17:17-18:3, 18:8-9. The “radio communication module is configured to utilize a secure identifier, and ... for two-way communication with a remote portable detection system.” *Id.* 18:1-3, 18:9-12. In this context, the claim term “secure identifier” is properly understood as “an identifier that identifies a connection for exchanging information between a UAV and a remote portable detection system, and that changes predictably to avoid spoofing and/or cloning of UAV transmissions across the connection, thereby providing a secure connection.”

In various embodiments, the '959 Patent discloses “systems and processes to provide secured wireless communication utilizing SSIDs.” *Id.*, 11:17-20. “By **frequently changing** the SSID, the probability of it being discovered and exploited or spoofed [is] greatly reduced.” *Id.*, 11:22-24. In general, “for this system to be reliable, the transmission of the [wireless connection] identification,” i.e., an identifier that identifies a connection, “must be reliable and unique, but also predictable to known parties so that the identification can be tracked ... to ensure that the wireless beacon was not changed or cloned, etc.” *Id.*, 11:25-29.

The '959 Patent makes it abundantly clear that a “*secure identifier*” is at the very heart of the advance taught and claimed by the '959 patent. The '959 Patent

starts by bemoaning the static connection identifiers used by conventional communication systems:

Encrypting information via a regular broadcast radio signal such as WiFi while utilizing a **static** SSID for the identification and addressing of WiFi packets is prone to “packet sniffing” to determine the SSID. Once the SSID is determined it may be possible to “clone” that device and intercept packets intended for it.

EX1001, 1:56-61.

Although the “Related Art” section of the ’959 Patent states that it “would be useful and more secure to have an encrypted identifier,” *id.*, 1:61-65, the ’959 Patent demonstrates that encrypting a connection identifier by itself is neither necessary nor sufficient to provide a “secure identifier” because it cannot provide two-way trust, and can be cloned. *See infra* at 9-11; *see also, id.*, 10:20-41 (identifying risks when communication occurs between **untrusted** UAVs and remote stations). As discussed below, the ’959 specification teaches that in a system with a two-way trust connection, a secure identifier must:

- (1) identify the connection between an authenticated or credentialed UAV and a detection system,
- (2) not be static, and instead,
- (3) should change, but predictably.

See id., 1:56-65, 10:20-11:4, 11:20-45.

Such an identifier allows the remote portable detection system to trust the UAV (and/or *vice versa*), so that “real-time peer-to-peer communication may be performed in a **secure manner**.” *Id.*, 11:7-11. And communication performed in a secure manner achieves the central objective of the ‘959 patent, which is establishing two-way trust in the communication between the UAV and the UAV detection system:

[T]here must be two-way trust between the server and the drone. For example, but not by way of limitation, the **drone must be able to trust that the server** that is transmitting policy information from a remote location such as at ground level **is authentic**, and is providing verified policy information. Conversely, **the server** and transmitters at the ground **must have trust that the target drone** that is receiving the policy information **is credentialed**. If two-way trust is not verified, the risk of transmission and reception is high.”

In light of this central teaching of the ‘959 Patent, that the communications between the UAV and UAV detection system must be “trusted,” it is no surprise that all examples of connection identifiers that are provided as embodiments of the invention in the ‘959 Patent, feature identifiers having the three aforementioned “secure identifier” features.

In particular, regarding non-static identifiers, the ‘959 Patent discloses **Example System 1** that “implements a **rotating SSID** which is utilized to address information packets over wireless networks. By **frequently changing the SSID**,

the probability of it being discovered and exploited or spoofed are greatly reduced. *Id.* 11:20-24. The '959 Patent also discloses **Example System 2** that uses “an OTP (one-time password) generation technique to periodically generate a token utilized for the SSID.” *Id.* 11:29-31.

Example System 3 includes an SSID generated using a “hash” or other “encryption or hashing methods.” *Id.* 11:32-39. Regarding Example System 3, the '959 Patent further states:

Because this hash is **immutable**, it must be **combined with another variable** [to] make sure that the **uniqueness** of the generated token **will be predictably different each time**. The system utilizes a digital time stamp at a given moment as the second portion of the information used to generate the token for the SSID.

Id., 11:40-45. Thus, the '959 Patent explains that a hash-based or encrypted SSID is “immutable,” i.e., static, and is not a secure identifier by itself. Only when a hash-based SSID is combined with a variable that is “predictably different each time,” e.g., a “digital timestamp,” can that SSID be utilized as a secure identifier.

In Example Systems 1-3, the SSIDs are non-static, i.e., they are rotated or change according to an OPT or a digital timestamp. The rotation or changes are made, however, in a manner that is predictable to both the UAV and the detection system, so that both systems can determine the SSID to be used at a certain time. If the SSIDs determined respectively by the UAV and the detection system match,

a connection identified by the matched SSID can be trusted by both systems, and recognized as a secure connection for exchanging information between the two systems. *See id.* 12:10-17 (“to establish wireless communications ... the SSID[s] ... must match,” which “allow[s] for **secure connection** between” a detection system and a UAV), 12:27-62 (describing UAVs using rotating SSIDs, OTP-based SSIDs, and timestamp-based encrypted SSIDs), FIGS. 9, 11-13.

Importantly, the ‘959 patent, and Example System 3 in particular, teach that Encrypting an identifier, by itself, does not convert it into a “secure identifier.” The reason is, an encrypted identifier can reduce the risk of unauthorized **changes** thereto and/or to a transmission via a connection identified by the encrypted identifier, but does **not prevent cloning** of the encrypted identifier and/or transmission. *See supra* at 33-35.

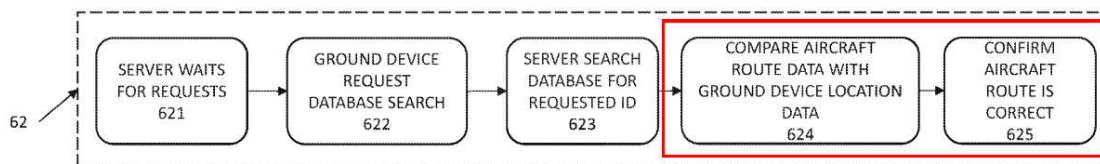
Example Systems 4 and 5 show that “secure identifiers” as construed above need not be SSIDs. Specifically, **Example System 4** of the ‘959 Patent includes “a ground device 21 [that] can detect aircraft[] through the RF signal transmitted from the” aircraft, e.g., a UAV. *Id.*, 6:31-33, FIGS. 2, 3A, 3B. The ‘959 Patent also states:

A location system antenna 27 (e.g., GPS antenna) is connected to a **location module 41** as antenna 40 in FIG. 4, in order to get the **position where the aircraft was detected**. Both information, including the detected id and the location detection position, are

transmitted to a server through a data communication antenna 28 connected to a data communication module 38 as antenna 34 in FIG. 4 (e.g. cellular network or Wi-Fi). The server will follow the aircraft **route confirmation process 62** as shown in FIG. 6, and reply an **id verification message** that is presented in the field 53 of the touchscreen 24.

Id., 6:20-30.

The route confirmation process 62 is reproduced and annotated below.



Id., FIG. 6 (partial, annotated). According to the “route confirmation process 62,” only if the location of the UAV that is detected by the location module 41 of the ground identification device 21 matches with the aircraft route data available to the server, the server can determine that the UAV “route is correct,” and thus, it is authenticated. Only upon such an authentication, the server may “reply an id verification message.” *Id.*, 6:23-30. Only upon receiving the “id verification message” the ground identification device 21 may “exchange information,” e.g., by initiating “duplex communication,” with the authenticated UAV. *Id.*, 6:59-67.

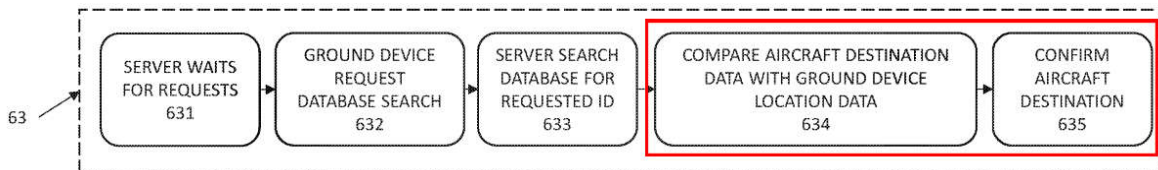
Example System 5 of the ’959 Patent includes “a delivery drone [that] can receive a message to update its destination coordinate[s] when it gets closer to the delivery address.” *Id.*, 7:3-5. Specifically:

The ground device 21 detects the UAV flying at a long distance from the user address through the RF signal received by the RF module 37. The **ground device 21 communicate[s] with the server sending the received ID and the device location capture[d] by the location module 41** (e.g., GPS, AGPS, Wi-Fi mapping or cellphone tower position) to check if the received id belongs to a delivery UAV going to the ground device position.

The server follows the **aircraft destination process flow 63** shown in FIG. 6 **to return the confirmation** to the ground device 21. When the server confirms [that] the UAV is going to the ground device position, the ground device 21 shows on its screen 24 a message informing the user that his delivery is arriving.

Id., 7:6-19, FIG. 6.

The aircraft destination process flow 63 is reproduced and annotated below.



Id., FIG. 6 (partial, annotated). According to the “aircraft destination process flow 63,” the server will determine that the UAV is authentic and headed to a designated destination only if the location of the UAV that is detected by the location module 41 of the ground device 21 at a given time matches with the aircraft destination data available to the server at that time,. Only upon such an authentication, will the server “return the confirmation to the ground device 21.” *Id.*, 7:14-16. After

receiving such conformation and thus confirming authentication of the UAV, “the ground device 21 will start to transmit its position through the RF module 37” “and the RF module 16 [of the UAV] receives the ground device 21 position.” *Id.*, 7:22-25. Thereafter, the ground identification device 21 may “exchange information,” e.g., by initiating “duplex communication,” with the authenticated UAV. *Id.*, 6:59-67.

To summarize, the identifier used for communications between the UAV and the UAV detection systems in each of Example Systems 1-5 meets the following requirement: “the identification must be reliable and **unique**, but also **predictable** to known parties so that the identification can be [] tracked on the server-side to ensure that the **wireless beacon was not changed or cloned**, etc.” *Id.* 11:25-29. In particular, in each of Example Systems 1-5, the identifier that is in use changes from time to time in a predictable manner. As a result, in all five Example Systems, if an unauthorized UAV sniffs a secure identifier from one transmission and attempts to reuse it in another, at a later time, the previously used identifier would not match the one expected at a later time, e.g., due to rotation or different OTP, timestamp, or changing UAV location.

Accordingly, in the context of Claim 21 and in light of the specification of the '959 Patent, the claim term “secure identifier” is properly interpreted as “an identifier that identifies a connection for exchanging information between a UAV

and a remote portable detection system, and that changes predictably to avoid spoofing and/or cloning of UAV transmissions across the connection, thereby providing a secure connection.”

IV. CLAIM 21 IS ENTITLED TO EARLIEST PRIORITY DATE OF JUNE 12, 2015

A. Claim 21 Is Entitled to Claim Priority to the '153 Provisional

The '959 Patent should be given the benefit of a claim of priority to the '153 Provisional because the subject matter of Claim 21 was fully supported as required by 35 U.S.C. § 112 in the '153 Provisional. In contending to the contrary, *see* Pet. at 7, Petitioner argues that the '153 Provisional does not provide adequate written description for” the limitation “secure identifier”² and that “the '153 Provisional does not use the term ‘identifier’ at all” *Id.* at 8. Specifically, Petitioner states that certain “identification codes” disclosed in the '153 Provisional “are not secure” and that the “'153 Provisional provides no discussion of securing the identification codes (e.g., by using encryption).” *Id.* at 9. Petitioner also states that “there is no discussion by the '153 Provisional of ‘securing’ anything.”” *Id.* These arguments are flawed, as discussed below.

First, the “test for determining compliance with the written description requirement is whether the disclosure of the application as originally filed

² Petitioner does not allege that the '153 Provisional does not adequately describe the other limitations of Claim 21. *See id.* at 7-9.

reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter, **rather than the presence or absence of literal support in the specification for the claim language.**” *Chiron Corp. v. Genentech, Inc.*, 363 F. 3d 1247, 1255 (Fed. Cir. 2004). Therefore, reciting “secure identifier” was not necessary to support fully Claim 21 in the ’153 Provisional.

Second, Petitioner misinterprets the claim term “secure identifier.” Petitioner appears to believe that encrypting an identifier converts the identifier into a “secure identifier.” *See* Pet. at 9. This is an error. In fact, as discussed under the Claim Construction section above, encryption is neither necessary nor sufficient for a “secure identifier.” *See supra* at 9-11 (Example Systems 1-3). Rather, a “secure identifier” is an identifier “that changes predictably to avoid spoofing and/or cloning of UAV transmissions” between a UAV and a detection system. *See supra* § III. And the ’153 Provisional discloses such secure identifiers.

Specifically, as discussed above in Claim Construction, Example Systems 4 and 5 of the ’959 Patent disclose a location of a UAV determined by a detection system, where authenticity of the UAV is verified using the determined location, and where a connection between the UAV and the detection system, for exchanging information, may be established upon the verification, as the claimed “secure identifier.” *See supra* at 14 (Example Systems 4-5)

The disclosure of Example Systems 4 and 5 in the '153 Provisional is substantially the same as that in the '959 Patent, as seen from a side-by-side comparison shown below. *See infra* at 26-31. Thus, the '153 Provisional “reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter,” i.e., a “secure identifier.” *Chiron Corp.*, 363 F. 3d 1255. The '153 Provisional adequately supports all of the other limitations recited in Claim 21, as well.³ *See generally*, EX1007. Therefore, Claim 21 is entitled to claim priority to the filing date of the '153 Provisional, i.e., June 12, 2015.

B. The '959 Patent Is Entitled to Claim Priority to the '071 PCT Application and to the '153 Provisional

1. The '959 Patent's Priority Chain is Not Broken and Meets the “Specific Reference” Requirement of 35 U.S.C. § 120

Petitioner argues that the “'959 Patent's priority chain contains a **fatal** error.” Pet. at 12. The priority chain identified U.S. Patent Application No. 15/839,661 (the '661 Application)⁴ as a “continuation” of International Patent Application No. PCT/US2016/037071 (the '071 PCT Application), where the correct identification would have been a “continuation-in-part.” *See* Pet. at 12, 14. Petitioner characterizes this error “fatal,” arguing that due to this error, the

³ Petitioner does not allege or argue otherwise. *See* Pet. at 7-9.

⁴ The '959 Patent issued from U.S. Patent Application No. 16/215,406, which is a continuation of the '661 Application. EX1001, face page, 1:7-9.

“specific reference to the earlier filed application” requirement of 35 U.S.C. § 120 is not met. *See* Pet. 10-12. As explained below, Petitioner misunderstands and/or misrepresents the applicable legal principles, and accordingly, Petitioner’s arguments are wrong.

For reference, the entire priority claim that the ’959 Patent recites in the specification is set forth below:

This application is a **continuation** of U.S. patent application Ser. No. **15/839,661** entitled LOW ALTITUDE AIRCRAFT IDENTIFICATION SYSTEM, filed on Dec. 12, 2017, which is a **continuation** of **PCT/US2016/037071** entitled A LOW ALTITUDE AIRCRAFT IDENTIFICATION SYSTEM, filed on Jun. 10, 2016, which **claims priority to** U.S. Provisional Patent Application No. **62/175,153**, entitled LOW ALTITUDE AIRCRAFT IDENTIFICATION SYSTEM, filed Jun. 12, 2015, all of which are incorporated herein by reference for all purposes. Further, U.S. patent application Ser. No. **15/839,661** **claims priority to** U.S. Provisional Patent Application No. **62/566,450**, entitled ENCRYPTION FOR LOW ALTITUDE AIRCRAFT IDENTIFICATION SYSTEMS, filed Oct. 1, 2017, which is incorporated herein by reference for all purposes.

EX1001, 1:7-22. In the recited priority claim of the ’959 Patent, no predecessor application of any of the patent applications in the entire priority chain of the ’959

patent is omitted, and each such predecessor application is identified by its correct serial number.

Petitioner relies on *Droplets, Inc. v. E* Trade Bank* to impugn the ‘959 patent’s priority chain.⁵ The patent at issue in *Droplets* (the ’115 Patent) claimed priority to a predecessor, the ’838 Patent, and incorporated it by reference. *See Droplets, Inc. v. E* Trade Bank*, 887 F. 3d 1309, 1316 (Fed. Cir. 2018). The ’838 Patent claimed priority to its predecessors, the ’745 Patent and the ’917 Provisional, but the ’115 Patent did not claim priority to the ’745 Patent and the ’917 Provisional. *See id.* The Board and the Federal Circuit both found that mere incorporation by reference of the ’838 Patent into the ’115 Patent did not meet the requirements of “a specific reference” under 35 U.S.C. § 120. *See id.* at 1316, 1320 (“§ 120’s ‘specific reference’ requirement does not contemplate incorporation by reference”).

Thus, in *Droplets*, the flaw in the priory chain of the ’115 Patent was not an error in mislabeling a familial relationship, *see* 887 F. 3d at 1315-16, but rather that the complete family was not disclosed. In that case, two predecessor applications were not expressly identified at all in the priority chain. *Id.* at 1312

⁵ Petitioner appears to cite *Droplets*, first on page 10 as “*Id.* at 1316” and then on page 11 as “*Droplets*, 887 F.3d at 1315,” neither of which is a complete, accurate citation.

(“the ’115 Patent **expressly claims priority only to** an immediately preceding application, and **not the provisional application** before that”). In this case by contrast, there is no such error in the priority claim of the ’959 Patent. The ’959 patent expressly claims priority to the ’711 PCT Application, and to all other predecessor patent applications in the priority chain.

Petitioner also states that the Board previously rejected “a priority claim in part because the priority claim misidentified itself as a divisional of the prior-filed application when it was not” Pet. at 11 (emphasis omitted) (citing *Apple Inc. v. e-Watch, Inc.*, IPR2015-00414, Paper 34 at 16-18 (PTAB 2016)). This argument appears to be based on a misunderstanding of *Apple*.

In *Apple*, the patent at issue, the ’168 Patent, which issued from the ’509 Application, was a continuation of the ’470 Application, which was a divisional application of the ’073 Application. IPR2015-00414, Paper 34 at 5-6. The cover page of the ’168 Patent identified the ’509 Application as a continuation of the ’470 Application. *Id.* at 7. The priority claim, however, did not include this identification; instead, the priority claim identified the ’509 Application as a divisional application of the ’073 Application. *See id.* at 7-8. The Board noted that “the ’509 application is not a divisional application of the earlier-filed ’073 application,” *id.* at 18, and that “the ’168 patent [failed] to correctly state the **relationships between the three applications**” *Id.* at 15. Accordingly, the Board

held that the '168 Patent “fail[ed] to ‘specifically reference’ the '073 application by correctly identifying its relationship to the '509 application.” *Id.*

Thus, in *Apple*, the recited priority claim of the '168 Patent failed to provide a “specific reference” not because the priority chain mislabeled a continuation application (“CON”) or a continuation-in-part application (“CIP”) as a divisional application (“DIV”), as Petitioner argues. *See* Pet. at 11. Rather, the Board found that “the correct relationship between the applications” was not identified, *see Apple* at 7-8, 16-17, because: (i) the '509 Application was not derived directly from the '073 Application, and as such, could not have been a DIV, CON, or CIP of the '073 Application; and (ii) though the '509 Application was a CON of the '470 Application, the priority claim did not mention the intervening '470 Application. None of these errors occur in the priority claim of the '959 Patent. Each and every patent application in the priority chain claims priority to all of its immediate predecessors, so that there is no missing, intervening patent application in any of the claimed priority chains in the '959 Patent.

To support its arguments, Petitioner also relies on *Medtronic*. *See* Pet. at 11. *Medtronic* held that “the ‘specific reference’ requirement mandates ‘each [intermediate] application in the chain of priority to refer to the prior applications.’” *Medtronic CoreValve v. Edwards Lifesciences Corp.*, 741 F. 3d 1359, 1363 (Fed. Cir. 2014) (quoting *Encyclopaedia Britannica, Inc. v. Alpine*

Electronics of America, Inc., 609 F.3d 1345, 1352 (Fed. Cir. 2010). In *Medtronic*, some intermediate applications failed to meet this requirement. *See id.* at 1362 (describing District Court findings that the priority claims of some intermediate applications (e.g., U.S. Applications 6 and 8) omitted other intermediate applications and thus “broke the priority chain” and “failed to link” all the intermediate applications), 1367 (affirming the District Court’s decision). Again, in ’959 Patent, there are no such errors in connection with the ’959 Patent. The respective priority chains of each of the intermediate patent applications is complete; there are no missing, intervening patent applications in the respective priority claims of any of the intermediate patent applications. *See* EX2001 at 2 (as required by PCT Art. 8, PCT Rule 4.10, and MPEP § 1828, the PCT Request for the ’071 Application does claim priority to the only predecessor thereof); EX1005, 1:7-14 (recites a priority claim identifying each and every predecessor application).

Per *Droplets*, “the specific reference [must] include each prior-filed application’s: (1) application number; and (2) familial relationship.” 887 F. 3d at 1315. In identifying the “familial relationship” in a patent, omission of one or more family members, i.e., predecessor application(s), in the priority claim, and/or identification of another patent application as an immediate (or non-immediate) predecessor when that other application is not an immediate (or non-immediate)

predecessor, can cause the patent to lose at least a partial claim of priority. *See Droplets* at 1312, 1315-16; *Apple* at 7-8; *Medtronic* at 1362.

Contrary to Petitioner's contention, *see* Pet. at 12, the '959 Patent's priority claim does not have these defects. An erroneous labeling of the relationship, e.g. CON instead of CIP or vice versa, is not fatal. *See Anascape, Ltd. v. Nintendo of America Inc.*, 601 F. 3d 1333, 1338 n.2 (Fed. Cir. 2010) (stating, while discussing whether a later-filed application contained new subject matter, where the designation of a predecessor was changed from CIP to CON, that "the designation given to a derivative application does not determine its legal status"). In *Transco Products*, in discussing requirements for disclosing the "best mode," the Court stated that "the expressions 'continuation,' 'divisional,' and 'continuation-in-part' are merely terms used for administrative convenience." *Transco Products Inc. v. Performance Contracting, Inc.*, 38 F. 3d 551, 556 (Fed. Cir. 1994) (citing MPEP § 201.11).

The version of the MPEP (Fifth ed., Rev. 16) ("MPEP-1994") that was applicable when *Transco Products* was decided is different from the version (Ninth ed., Rev. 8) (MPEP-2018) that was applicable when the application for the '959 Patent was filed. *See* EX2002. For instance, unlike MPEP-1994, MPEP-1998 does not state that "the name used is immaterial, the names being merely expressions developed for convenience." *Compare* EX2003 § 201.11 (Section

“Copendency”) with EX2004 § 211.01(b) (Section “Copendency”); *see also Pfizer, Inc. v. Teva Pharmaceuticals USA, Inc.*, 518 F. 3d 1353, 1360, 1362 (finding that for the purposes of 35 U.S.C. § 121, DIV applications have different rights from CON and CIP applications).

Regarding the right to claim priority, however, both MPEP-1994 and MPEP-2018 state that the “term ‘continuity’ is used to express the relationship of copendency of the same subject matter in two different applications,” that the second or later-filed “application may be referred to as a continuing application,” and that “[c]ontinuing applications include” “division[s / al], continuation[s], and continuation-in-part” applications. EX2003 § 201.11 (Section “Copendency”); EX2004 § 211.01(b) (Section “Copendency”). Both MPEP-1994 and MPEP-2018 also state: that the “statute is so worded that the first application may contain more than the second, or the second application may contain more than the first, and in either case the second application is entitled to the benefit of the filing date of the first as to the common subject matter.” EX2003 § 201.11; EX2004 § 211.01(b).

Consistent with the MPEP, in *Transco Products*, the Court stated that “the bottom line is that, no matter what term is used to describe a continuing application, that application is entitled to the benefit of the filing date of an earlier application only as to common subject matter.” *Transco Products*, 38 F. 3d at 556. As discussed below (and above, *see supra* § IV.A), the ’406 Application, the ’071

PCT Application, and the '153 Provisional include common subject matter that fully supports Claim 21.⁶ Therefore, Claim 21 is entitled to claim priority to both the '071 PCT Application and the '153 Provisional. Accordingly, in the '959 Patent, the labeling of the '071 PCT Application as CON is not fatal, and the priority chain of the '959 Patent is not broken.

2. Claim 21 Is Entitled to Claim Priority to the '071 PCT Application

Claim 21 is entitled to claim priority to the '071 PCT Application because the '071 PCT Application discloses the subject matter of Claim 21 as required by 35 U.S.C. §112. In contending otherwise, *see* Pet. at 10, 12, Petitioner argues that the '071 PCT Application does not provide adequate written description for” the limitation “secure identifier”⁷ and that the '071 PCT Application “does not use the term ‘identifier’ at all” *Id.* at 14. Specifically, Petitioner states that certain “identification codes” disclosed in the '071 PCT Application “are not secure” and that the “'071 [PCT] Application provides no discussion of securing the identification codes (e.g., by using encryption).” *Id.* at 15. Petitioner also states

⁶ The common subject matter is also disclosed in the intervening '661 Application, and Petitioner does not allege otherwise. *See* Pet. at 7-16.

⁷ Petitioner does not allege that the '153 Provisional does not adequately describe the other limitations of Claim 21. *See id.* at 7-9.

that the '071 PCT Application “includes no discussion of ‘securing’ anything.”

Id. These arguments are flawed, as discussed below.

As discussed for the '153 Provisional, “literal support in the specification for the claim language” is not needed, *Chiron Corp.*, 363 F. 3d at 1255, and Petitioner misinterprets the claim term “secure identifier.” *See supra* at 15-16. Moreover, as discussed above in Claim Construction, Example Systems 4 and 5 of the '959 Patent fully support the claimed “secure identifier.” *See supra* at 11-14. The disclosure of Example Systems 4 and 5 in the '071 PCT Application is substantially the same as that in the '959 Patent, as seen from a side-by-side comparison below.

Example System 4

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
“a ground device 21 [that] can detect aircraft[] through the RF signal transmitted from the” aircraft, e.g., a UAV. 6:31-33, FIGS. 2, 3A, 3B.	“a ground device to assist the aircraft identification” where the “device has [an] RF receiver capable of receiving the identification box RF signal [from a UAV] to	“a remote (e.g. ground) device to assist the aircraft identification” where the “device has an RF receiver capable of receiving the identification box RF signal [from a UAV] to connect both information

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
	cross both information ⁸ and verify the authenticity” of the UAV. Pp. 10-11.	sources and to verify the authenticity” of the UAV. ¶[16].
“A location system antenna 27 (e.g., GPS antenna) is connected to a location module 41 as antenna 40 in FIG. 4, in order to get the position where the aircraft was detected . Both information, including the detected id and the location detection position, are transmitted to a server The server will follow the aircraft route confirmation process 62 as shown in FIG. 6, and	A location system antenna 27 (e.g., GPS antenna) is connected to a location module 41 in order to get the position where the aircraft was detected . Both information, the detected ID and the location detection position, are transmitted to a server The server will follow the aircraft route confirmation process 62 and reply with an ID verification message that is presented in the	“A location system antenna 27 (e.g., GPS antenna) is connected to a location module 41 as antenna 40 in FIG. 4, in order to get the position where the aircraft was detected . Both information, including the detected id and the location detection position, are transmitted to a server The server will follow the aircraft route confirmation process 62 as shown in FIG. 6, and

⁸ The information captured by a camera of the ground device and that received by the RF receiver of the ground device. EX1007 at 10-11.

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
reply an id verification message that is presented in the field 53 of the touchscreen 24.” <i>Id.</i> , 6:20-30.	field 53 of the touchscreen 24. P. 13.	reply an id verification message that is presented in the field 53 of the touchscreen 24.” ¶[39].
 FIG. 6 (partial, annotated).	 P. 22 (annotated).	 FIG. 6 (partial, annotated).
“The RF receiver and transmitter 16 and 37 in both the identification box 1 and the ground device 21 creates a duplex communication. Therefore, the identification box 1 and ground device 21 together can exchange information through light or RF.” 6:59-67.	The RF receiver and transmitter 16 and 37 in both devices also creates a duplex communication. Therefore, the identification box 1 and ground device 21 together can exchange information through light or RF. P.13.	“The RF receiver and transmitter 16 and 37 in both the identification box 1 and the ground device 21 creates a duplex communication. Therefore, the identification box 1 and ground device 21 together can exchange information through light or RF.” ¶[43].

Example System 5

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
“a delivery drone [that] can receive a message to update its destination coordinate[s] when it gets closer to the delivery address.” <i>Id.</i> , 7:3-5.	“a delivery drone [that] can receive a message to update its destination coordinate[s] when it get[s] closer to the delivery address.” Pp. 13-14.	“a delivery drone [that] can receive a message to update its destination coordinate[s] when the delivery drone gets closer to the delivery address.” ¶[44].
“The ground device 21 detects the UAV flying at a long distance from the user address through the RF signal received by the RF module 37. The ground device 21 communicate[s] with the server sending the received [UAV] ID and the device location capture[d] by the location module 41 (e.g., GPS, AGPS, Wi-Fi mapping or cellphone	The ground device 21 detects the UAV flying at a long distance from the user address through the RF signal received by the RF module 37. The ground device 21 communicates with the server sending the received [UAV] ID and the device location measured by the location module 41 (e.g., GPS, AGPS, Wi-Fi mapping or cellphone	“The ground device 21 detects the UAV flying at a long distance from the user address through the RF signal received by the RF module 37. The ground device 21 communicates with the server sending the received [UAV] ID and the device location capture[d] by the location module 41 (e.g., GPS, AGPS, Wi-Fi mapping or cellphone

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
tower position) to check if the received id belongs to a delivery UAV going to the ground device position.” 7:6-13.	tower position) to check if the received ID belongs to a delivery UAV going to the ground device position. P. 14.	tower position) to check if the received id belongs to a delivery UAV going to the ground device position. ¶[44].
“The server follows the aircraft destination process flow 63 shown in FIG. 6 to return the confirmation to the ground device 21. When the server confirms [that] the UAV is going to the ground device position, the ground device 21 shows on its screen 24 a message informing the user that his delivery is arriving.” 7:14-19, FIG. 6.	The server follows the aircraft destination process flow 63 in order to return the confirmation to the ground device 21. When the server confirms if the UAV is going to the ground device position, the ground device 21 shows on its screen 24 a message informing the user that his delivery is arriving. P. 14.	“The server follows the aircraft destination process flow 63 shown in FIG. 6 to return the confirmation to the ground device 21. When the server confirms if the UAV is going to the ground device position, the ground device 21 shows on its screen 24 a message informing the user that his delivery is arriving.” ¶[45], FIG. 6.
 FIG. 6 (partial, annotated).	 P. 22 (annotated).	 FIG. 6 (partial, annotated).

Disclosure from the '959 Patent (EX1001)	Corresponding Disclosure from the '153 Provisional (EX1007)	Corresponding Disclosure from the '071 PCT Application (EX1006)
“the ground device 21 will start to transmit its position through the RF module 37” “and the RF module 16 [of the UAV] receives the ground device 21 position.” 7:22-25.	“the ground device 21 will start to transmit its position through the RF module 37” “and the RF module 16 [of the UAV] receives the ground device 21 position.” P. 14.	“the ground device 21 will start to transmit its position through the RF module 37” “and the RF module 16 [of the UAV] receives the ground device 21 position.” ¶[46].
“the UAV will update its destination to drop the delivery in the exact location the user [i.e., the ground device 21] is transmitting.” <i>Id.</i> , 7:28-30.	“the UAV will update its destination to drop the delivery in the exact location the user [i.e., the ground device 21] is transmitting.” P.14.	“the UAV will update its destination to drop the delivery in the exact location the user [i.e., the ground device 21] is transmitting.” ¶[046].

Thus, the '071 PCT Application “reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter,” i.e., a “secure identifier.” *Chiron Corp.*, 363 F. 3d 1255. The '071 PCT Application adequately supports all of the other limitations recited in Claim 21, as well.⁹ *See*

⁹ Petitioner does not allege or argue otherwise. *See* Pet. at 14-16.

generally, EX1006. Therefore, Claim 21 is entitled to claim priority to the filing date of the '071 PCT Application.

In summary, because the priority chain of the '959 Patent is not broken, *see supra* § IV.B.1, and because the '071 PCT Application claims priority to the '153 Provisional, Claim 21 is entitled to claim priority to the filing date of the '071 PCT Application, June 10, 2016, and further, to the filing date of the '153 Provisional, i.e., June 12, 2015.

V. EACH OF GROUNDS 1-4 FAILS TO DEMONSTRATE UNPATENTABILITY OF CLAIM 21 BY A PREPONDERANCE OF THE EVIDENCE

A. Ground 1

In Ground 1, Petitioners rely on a flawed allegation regarding the priority date as shown above, and an improper interpretation of “secure identifier” that effectively reads out this limitation from Claim 21. Petitioner considers “October 1, 2017, the filing date of U.S. Provisional Application No. 62/566,450, to which the '959 and '451 Patents claim priority” as the priority date of the '959 Patent.” Pet. at 15-16; *see id.* at 16 n.3. The actual filing date of Beard (EX1008) is February 26, 2018. EX1008, face page; Pet. at 16. Thus, it is undisputed that Beard, by itself, is not prior art.

Beard claims priority to several non-provisional and provisional patent applications. *See* EX1008, 1:20-2:13. Petitioner states that “Beard claims priority to U.S. Provisional Application No. 62/480,031 (EX1009, ‘Beard Provisional’)

filed on March 31, 2017” and that “the subject matter relied upon in Beard is disclosed in Beard Provisional.” Pet. at 16. As discussed above, the ’959 Patent is entitled to its earliest claimed priority date of June 12, 2015. *See supra* § IV. Therefore, Beard Provisional is also not prior art. Accordingly, as a threshold matter, Beard by itself and through Beard Provisional does not qualify as prior art.

Even if assuming, for the sake of argument, that the Beard Provisional qualified as prior art, it does not teach each and every limitation of Claim 21. Specifically, contrary to Petitioner’s allegation, *see* Pet. at 34-35, Beard Provisional’s “digital signature” is not the claimed “secure identifier.”

Specifically, Beard Provisional discloses that the “digital signature” is “a TLS/SSI AirMap Drone ID signature.” EX1009 at 19. A TLS/SSI signature is a digitally signed, encrypted public-key certificate. *See* EX2005 at 1, 5-6; EX2006 at 1, 6, 9-10. Such a certificate and the Drone ID do not change from time-to-time, and as such, Beard Provisional does not disclose that its “digital signature” can change predictably, to avoid spoofing and/or cloning of UAV transmissions across the connection. This means that Beard Provisional’s digital signature is just like the conventional identifiers bemoaned in the ’959 Patent as failing to address the risk of spoofing via sniffing, and does not provide a secure connection. *See* EX1001, 1:56-61.

It is noted that Beard Provisional describes its digital signature as “anti-spoofing.” EX1009 at 18, 25. The anti-spoofing protection provided by Beard Provisional’s digital signature, however, can only ensure that the underlying Drone ID was not changed / hacked. *See* EX2005 at 13 (“PKI certificates help to ensure that a drone’s identity can be trusted and has not been spoofed or hacked”); EX2006 at 10. Beard Provisional’s signature does not ensure that the signature, the Drone ID, and/or the UAV transmissions have not cloned.

Such cloning or spoofing and unauthorized use of the clone/spoofed copy are known as a “replay attack.” *See* EX2007 at 187 (“‘replay’ [means] the capture of a message or a piece of a message that is then used at a later time”). Syverson (EX2007) describes replay attacks in a wide range of applications, and when describing a financial transaction application, explains that encryption does not prevent replay attack. In describing “a very clear form of replay attack,” Syverson states:

Suppose that Ann authorizes a transfer of funds from one account to another by **encrypting the transfer request with a signature** key known only to her. To get this processed she then sends it to a machine that checks the signature and performs the transaction. If a **penetrator**, Eve, wished to have the same **transfer repeated** without Ann's knowing authorization, she would not need to be able to produce the encrypted transfer request herself. Assuming she can guess or otherwise determine which message text corresponds to the

transfer request, she need only **eavesdrop a copy of the encrypted request and then replay it** at another time.

Id. (footnote omitted); *see* EX2008 at 2-3 (“A replay attack is an attack where an adversary records messages between two parties and can later replay any of those messages to either party member as though it was sent legitimately. The **attacker does not need to know what the message decrypts to** in order to send it.”).

Thus, a digital signature, such as Beard Provisional’s, does not protect against a replay attack, in which an unauthorized entity, e.g., an unauthorized UAV, can eavesdrop on a communication between an authorized UAV and a detection system, and copy and clone the encrypted digital signature. Using the cloned signature in a later transmission, the unauthorized UAV can masquerade as the authorized UAV. Indeed, EX- Syverson states that “[s]omething is needed to guard against such replay, **in addition to** a good encryption algorithm.” EX- Syverson at 187.

Therefore, a digital signature, such as Beard Provisional’s, unlike the “secure identifier” of Claim 21, cannot avoid cloning because the identifier fails to “change predictably” from time-to-time. With the ’959 Patent’s secure identifier, the UAV and/or the detection system would expect the subsequent connection / transmission to have its own unique secure identifier that is different than the one previously used by the system. This way, if the same identifier is received in a subsequent

transmission, cloning can be detected. Beard Provisional's digital signature is static however, and does not and cannot prevent such replay attacks. Therefore, Beard Provisional does not teach or suggest a "secure identifier," i.e., an identifier "that changes predictably to avoid spoofing and/or cloning of UAV transmissions, thereby providing a secure connection," for exchanging information, per a proper interpretation of "secure identifier." *See supra* § III.

In addition, a POSITA would not implement digital signatures that are computationally intensive cryptographic operations on a UAV with limited computing and bandwidth capabilities. In the context of protecting against injury or damage from an unauthorized UAV, secured identifiers need to be swiftly generated and processed while remaining unique. Digital signatures, in contrast, are computationally too intensive to meet this requirement.

In summary, Beard / Beard Provisional do not qualify as prior art, and regardless, do not teach or suggest each and every limitation of Claim 21. Therefore, Beard and/or Beard Provisional do not anticipate or render obvious Claim 21.

B. Ground 2

1. A POSITA Would Not Combine Taveira, Wang, and Gong

A POSITA would not combine Taveira, Wang, and Gong because, *inter alia*, that combination (the "Taveira-Wang-Gong combination"): (i) "would produce an

inoperative result,” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F. 3d 1314, 1326 (Fed. Cir. 2009), and (ii) does not provide a reasonable expectation of achieving the claimed invention. *Intelligent Bio-Systems v. Illumina Cambridge*, 821 F. 3d 1359, 1367 (Fed. Cir. 2016); *Personal Web Technologies, LLC v. Apple, Inc.*, 848 F. 3d 987, 993-94 (Fed. Cir. 2017); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015).

Petitioner first argues that a POSITA would combine Taveira’s and Wang’s teachings so that certain spoofing-prone identifiers that Taveira discloses, namely, SSIDs and MAC addresses, “are encrypted as taught by Wang (e.g., using ‘SSID hiding’ and ‘MAC ID filtering’).” *See* Pet. at 40, 53-54. This argument is flawed because it ignores certain pertinent aspects of Taveira, including the one stated in the very sentence in which Taveira mentions SSID and MAC addresses.

In particular, Taveira discloses that its drone “may be configured to receive navigation signals,” e.g., “from recognizable RF emitters (e.g., AM/FM radio stations, WiFi access points, and cellular network base stations) on the ground.” EX1010, ¶[0056]. “The locations, unique identifiers ... of such RF emitters may be stored in a database and used to determine position ... when RF signals are received.” *Id.* Taveira further states: “upon receiving an RF signal via the radio module 130, the processor 120 may obtain the signal[']s unique identifier (e.g., a service sector identification (SSID), a media access control (MAC) address, radio

station call sign, cell ID, etc.), and use that information to obtain the ground coordinates and signal strength of the detected RF emitter from the database of RF emitter characteristics.” *Id.* Taveira also states: “Estimates of location based on received ground based RF emitters may be combined with position information from a GNSS receiver to provide more precise and reliable location estimates than achievable with either method alone.” *Id.*

Thus, Taveira describes receiving signals from ground-based RF emitters **not to facilitate secure communication with drones, but rather to determine the drone’s location more accurately and reliably.** In Taveira, an RF emitter’s identifier is obtained from an RF signal received from the emitter, and that identifier is used to obtain the ground position of the emitter from a database. The emitter’s ground position can then be used to determine the drone’s position accurately. *See id.*

The ability to perform such emitter-signal-based location determination would be **reduced significantly, however, if not disabled entirely,** in the combination of Taveira and Wang (the “Taveira-Wang” combination) that Petitioner proposes. This is because by applying Wang’s encryption “using ‘SSID hiding’ and ‘MAC ID filtering,’” *see* Pet. at 40, 53-54, Taveira’s emitter-signal-based location determination is compromised. If Wang’s MAC address filtering is employed in Taveira, the drone’s processor 120 would ignore signals received from

all emitters / ground stations having unknown MAC addresses, e.g., from stations with which the drone is not configured to communicate. EX2009 at 107 (MAC Address filtering “only allow[s] devices with specific MAC addresses to connect”). This would substantially mitigate Taveira’s ability to perform location determination, which is the only use Taveira makes of its identifiers, because the triangulation / trilateration method used by Taveira for location determination requires at least three signals having three identifiers for each instance of location determination, and a filtered out MAC address cannot be used in such location determination. *See id.*

Likewise, if Wang’s SSID hiding is employed in Taveira, the location determination using RF emitters employing SSID hiding would become infeasible. This is because, the drone’s processor 120 would not detect the hidden SSID, i.e., the RF emitter’s identifier, and cannot therefore obtain the emitter’s position from the database. It should be noted that the very sentence in which Taveira describes that a drone may obtain an emitter’s SSID or MAC address, it discloses “us[ing] that information to obtain the ground coordinates ... of the detected RF emitter from the database of RF emitter characteristics.” *Id.* As discussed above, this cannot be accomplished, at least in substance, in the proposed combination, and “would produce an inoperative result.” *DePuy*, 567 F. 3d at 1326 (quoting *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1382 (Fed. Cir. 2007)).

Petitioner also argues that “Taveira itself provides a motivation to combine with Wang[.]” Pet. at 21. In particular, Petitioner states that Taveira describes its drones as susceptible to “‘tampering,’ intercepting, ... hijacking,” and discloses that certain “‘identifying information may [] be encoded to prevent or discourage tampering or spoofing.” Pet. at 41 (quoting EX1010, ¶¶[0002], [0091]).

Therefore, Petitioner argues, a POSITA would have looked to Wang’s solution of encryption of signals. *See id.* A POSITA would not have been motivated to do so for at least three reasons. First, as discussed above, encoding / encrypting an identifier does not convert such an identifier into a “secure identifier.” *See supra* at 33-35. A POSITA would have also understood that the prevention / discouragement of spoofing of the identification information that Taveira describes are only partial, in that tampering with the encoded identification information or replacing it with another may be prevented. But, as described above, an encoded / encrypted identifying information and a heart beat signal containing such information, can nevertheless be cloned. *See supra* at 33-35.

Second, a POSITA would have understood that the combination would not have addressed the stated threat in the ‘959 patent of avoiding cloning of transmissions between a UAV and a detection system. Petitioner ignores key context from Taveira, and the proposed combination provides no expectation at all of achieving the Claim 21’s “secure identifier.” As explained below, the

identifying information that may be encoded is transmitted in a “heart beat signal.”

See infra at 47-49. In Taveira, the heart beat signal is used to ensure that the system is “functioning correctly” and/or a connection between a drone and a station is “maintained and [is] viable.” *See id.*; EX1010 ¶¶[0043], [0066]. The heart beat signal is not used for exchanging data between a UAV and a detection system. *See infra* at 47-49. As such, a POSITA would have readily understood that encoding or encrypting the identifying information in a heart beat signal as Wang teaches would not alter the communication / connection between a UAV and a control / detection system at all, and would not improve the security of such communication. Therefore, a POSITA would have understood that the proposed combination would not have solved the problems that Taveira notes, such as tampering, intercepting, hijacking, etc., of drones.

As such, the proposed combination provides no expectation at all of achieving the claimed “secure identifier.” *See supra* § III; *infra* at 47-49.

Third, Petitioners allege that combining Wang’s encryption techniques and Taveira’s communications between a drone and another device would yield the predictable result of “producing a wireless communication system that utilizes encrypted communications.” Pet. at 42. The ’959 Patent is not directed to this mere “encryption” result however, as discussed above, and describes the inadequacy of such a technique:

Encrypting information via a regular broadcast radio signal such as WiFi while utilizing a static SSID for the identification and addressing of WiFi packets is prone to “packet sniffing” to determine the SSID. Once the SSID is determined it may be possible to “clone” that device and intercept packets intended for it.

EX1001, 1:56-61.

The '959 Patent teaches that encrypting an identifier is neither necessary nor sufficient to provide a “secure identifier.” Rather, a non-static, predictably changing connection identifier is needed. *See supra* at 9-11.

Therefore, by combining Wang with Taveira, a POSITA would have no expectation at all of “achieving what is claimed” in the '959 Patent. *Intelligent Bio-Systems*, 821 F. 3d at 1367; *Personal Web Technologies*, 848 F. 3d at 993-94 (quoting *Belden Inc.*, 805 F.3d at 1073).

For the foregoing reasons, a POSITA would not combine Taveira and Wang, along with Gong. Notwithstanding the lack of motivation to combine, the Taveira-Wang-Gong combination fails to teach or suggest all of the limitations of Claim 21, as discussed below.

2. The Taveira-Wang-Gong Combination Does Not Teach or Suggest “a Secure Identifier” Recited in Claim 21

a) A Hidden SSID and a Filtered MAC Address Are Not “Secure Identifier[s]”

Encrypting Taveira’s identifiers such as SSID and MAC address, “using SSID hiding or MAC ID filtering as taught by Wang,” *see* Pet. at 53-54, does not teach or suggest “a secure identifier,” as discussed below. As a threshold matter, a POSITA would not combine Taveira and Wang to apply Wang’s encryption to Taveira’s SSID / MAC address, because doing so would make these identifiers unsuitable for their intended and stated purpose of location determination. *See supra* § V.B.1.

Moreover, as discussed above, Taveira uses the SSID and/or MAC address of an RF emitter “to provide more precise and reliable location estimates.” *See supra* at 37-38; EX1010, ¶[0056]. The SSID and/or MAC address do not establish a connection for exchanging information between a drone and the RF emitter, such as the communication link 132 or the connection 232. *See* EX1010, ¶¶[0057], [0063], FIGS. 1, 2A, 2B.

Even if Taveira’s SSID and/or MAC address are modified according to Wang, the hidden SSID and/or filtered MAC address / ID would not be “an identifier that identifies a connection for exchanging information between a UAV

and a remote portable detection system,” as a proper interpretation of “a secure identifier” requires. *See supra* § III.

As discussed above, encrypting an identifier is neither necessary nor sufficient to provide a “secure identifier.” *See supra* at 9-11. Rather, a “secure identifier” is properly understood as an identifier “that changes predictably to avoid spoofing and/or cloning of UAV transmissions across [a] connection” between a UAV and a detection system. *See supra* § III. As discussed below, Taveira’s identifiers, modified per Wang as Petitioner proposes, are static, and hence, do not meet the above-identified requirements of “a secure identifier.”

First, a hidden SSID is still a static SSID, i.e., it does not change from time-to-time. Petitioner, Dr. Chowdhary, Taveira, and Wang do not state or suggest otherwise. *See* Pet. at 40-60; EX1003, ¶¶138-171; *see generally*, EX1010; EX1011. Therefore, a hidden SSID is not “an identifier “that changes predictably.”

Second, the ’959 Patent explains that a static SSID can be sniffed, i.e., discovered, and thereupon, it can be cloned. EX1001, 1:56-61. In a like manner, a hidden SSID, despite being hidden, can also be discovered easily, and then cloned. This is because, when the SSID is hidden, to establish a two-way communication, the UAV or the detection system must broadcast the hidden SSID periodically, where well-known techniques / tools can be used to discover the so-called hidden SSID, which can then be cloned.

For example, Cunche-1 (EX2010) explains that the “active service discovery mode is required in the case of wireless networks with a hidden SSID,” and in that mode the devices “continuously broadcast probe request messages” from which “an eavesdropper can easily collect the set of announced SSID[s].” EX2010 at 2-3. Lindqvist (EX2011) describes that “disabling the SSID broadcast has the **unintended consequence** that the client stations go around **broadcasting** Probe Requests containing **the SSID**” where it is not hidden. EX2011 at 3.

Therefore, in the proposed Taveira-Wang-Gong combination, the hidden SSID can be easily detected and cloned, and would not “avoid spoofing and/or cloning of UAV transmissions” between a UAV and a detection system. Such a hidden SSID is therefore not be the claimed “secure identifier.”

Wang’s MAC ID / address filtering, which can provide some “protection by only allowing devices with specific MAC addresses to connect,” EX2009 at 107, suffers from the same shortcomings discussed above. In particular, the specified MAC addresses are static, and can be detected easily and then used for spoofing, e.g., by cloning. *See, e.g.*, EX2012 at 1 (even “if the payload of some Wi-Fi frames can be encrypted, the header is always transmitted in clear” so “the MAC address of the devices ... can be collected”); EX2013, Abstract (“In the networks that use MAC address based filtering approach to authenticate the clients, the spoofer just needs to get a valid MAC address that belong to some authorized

client in the network in order to gain an illegitimate advantage”), 1770 (the “most common spoofing attacks are **MAC address spoofing** and IP address spoofing).

Thus, in the proposed Taveira-Wang-Gong combination, a filtered MAC address / ID is static, and can be easily detected and cloned, and is therefore not an identifier “that changes predictably to avoid spoofing and/or cloning of UAV transmissions” between a UAV and a detection system. Hence, such a filtered MAC address / ID is also not the claimed “secure identifier.”

b) Encrypted Drone Information Is Not a “Secure Identifier”

Encrypting Taveira’s “transmitted drone information” “as taught by Wang,” *see* Pet. at 54-55, also does not teach or suggest a “secure identifier.” As described above, encryption alone does not convert an identifier into a “secure identifier.” *See supra* at 33-35. Rather, “to avoid spoofing and/or cloning of UAV transmissions” between a UAV and a detection system, a “secure identifier” must be an identifier “that changes predictably.” *See supra* § III. The proposed combination does not teach or suggest this limitation.

Specifically, Taveira discloses that “drone information” provided to “an access server” (to the extent such an access server is a detection system), may include “a drone identifier, a drone access level, drone payment information, drone authorization credentials, and/or other information.” EX1010, ¶[0110]; *see id.*,

¶[0117]. This information is either static, e.g., the drone identifier, or to the extent it may change, it does not change predictably, i.e., in a manner in which the access server can predict the new, changed information. Encryption, as taught by Wang, does not change these aspects of the drone information. As such, Taveira’s drone information, regardless of encryption, does not include an identifier “that changes predictably to avoid spoofing and/or cloning of UAV transmissions” between a UAV and a detection system. *See supra* § III. Therefore, Taveira’s drone information, when encrypted, is not and does not teach or suggest the claimed “secure identifier.”

c) Encoded Identifier in a Heart Beat Signal Is Not a “Secure Identifier”

Taveira’s “heart beat signals” that may include “a device identifier [or] other identifier” that may be “encoded to prevent or discourage tampering or spoofing,” *see Pet.* at 55 (citing EX1010, ¶¶[0091]-[0092]), is also not the claimed “secure identifier,” as discussed below.

Taveira states that “the drone may be configured to sense a heart beat signal from the server and/or vice versa that is indicative of systems functioning correctly.” EX1010, ¶[0043]. “For example, the drone 100 may receive [or send] periodic communications from [or to] the server 240 indicating that the connection 232 is still maintained and viable” or “indicating that the navigation unit 125 and

other drone systems are still functioning.” *Id.*, ¶[0066]. Taveira also discloses different ways in which “tampering or spoofing” of the heart beat signals can be prevented or discouraged. *See e.g., id.* ¶[0091] (using “a prearranged frequency schedule,” “encoding” the signal, including “device identifier” of the “sending system” or [an]other identifier” that may be encoded).

Thus, Taveira’s heart beat signal is not used to exchange information between a drone and a device sending the heart beat signal. Rather, the heart beat signal can ensure that a different, associated connection that may be used to exchange information, e.g., the connection 232, and/or the drone system are viable or are functioning correctly. Therefore, to the extent Taveira’s encoded identifier may prevent tampering or spoofing of the identifier and/or the heart beat signal carrying the encoded identifier, that identifier does not “identif[y] a connection for exchanging information between a UAV and a remote portable detection system,” as a proper interpretation of “a secure identifier” requires. *See supra* § III. For that reason, the encoded identifier does not and cannot prevent tampering or spoofing of the different connection, e.g., the communication link 132 or the connection 232. *See* EX1010, ¶¶[0057], [0063], FIGS. 1, 2A, 2B.

Moreover, as discussed before, encoding / encrypting a device or another identifier does not convert such an identifier into a “secure identifier.” *See supra* at 33-35. A POSITA would have understood that the prevention / discouragement of

spoofing that Taveira describes are only partial, in that tampering of the encoded identifier and/or replacing the encoded identifier with another may be prevented. But, as described above, an encoded / encrypted identifier and a heart beat signal containing such a message, can nevertheless be cloned. *See supra* at 33-35. To “avoid spoofing and/or cloning of UAV transmissions” between two devices or systems, a “secure identifier” must be an identifier “that changes predictably,” and must also be an “an identifier that identifies a connection” between those two systems. *See supra* § III. Taveira’s encoded identifying information in the heart bear signal is not such an identifier, and as such, Taveira’s use of the heart beat signals does not teach or suggest “a secure identifier.”

Petitioner does not contend in the proposed combination that Gong teaches or suggests “a secure identifier,” *See Pet.* at 53-55. Thus, in summary, Taveira, Wang, and Gong, individually or in combinations as proposed, do not teach or suggest “a secure identifier,” and thus fail to teach all of the limitations of Claim 21. Accordingly, the Taveira-Wang-Gong combination does not render Claim 21 obvious.

C. Ground 3

1. A POSITA Would Not Combine Taveira, Qi, and Gong

A POSITA would not combine Taveira, Qi, and Gong because, *inter alia*, that combination (the “Taveira-Qi-Gong combination”): (i) “would produce an

inoperative result,” *DePuy Spine*, 567 F. 3d at 1326, and (ii) does not provide a reasonable expectation of achieving the claimed invention. *Intelligent Bio-Systems*, 821 F. 3d at 1367; *Personal Web Technologies*, 848 F. 3d at 993-94; *Belden*, 805 F.3d at 1073.

Petitioner argues that Taveira describes its drones as susceptible to “‘tampering,’ intercepting, ... hijacking,” and hence, a POSITA would have understood that Taveira’s “SSID or MAC address” can be updated periodically “as taught by Qi[,] to reduce the likelihood of an attacker to discover the SSID or MAC address and use it for illicit purposes.” Pet. at 60-61 (quoting EX1010, ¶¶[0002]). Petitioner also argues that such a modification would have been “merely combining prior art elements ... [by] known methods ... to yield predictable results.” *Id.* at 61. These arguments are wrong because they ignore certain pertinent aspects of Taveira, including the one stated in the very sentence in which Taveira mentions SSID and MAC address. *See supra* at 37-38 (discussing a similar flaw in Petitioner’s Taveira-Wang combination).

Taveira’s drones “receive navigation signals,” “from recognizable RF emitters ... on the ground.” EX1010, ¶[0056]. A “signal[’]s unique identifier (e.g., a service sector identification (SSID), a media access control (MAC) address, ... , etc.),” is used “to obtain the ground coordinates ... of the detected RF emitter from” a database that stores the “RF emitter characteristics” such as the “locations,

unique identifiers ... of such RF emitters.” *Id.* The database may be “stored in the onboard memory” of the drone or in a “Location Information Service (LIS) server.” *Id.* Taveira also states: “Estimates of location based on received ground based RF emitters may be combined with position information from a GNSS receiver to provide more precise and reliable location estimates than achievable with either method alone.” *Id.*; *see supra* at 37-38.

Thus, Taveira describes receiving signals from ground-based RF emitters not to communicate with them but to determine the drone’s location more accurately and reliably. To this end, an RF emitter’s identifier is obtained from an RF signal received from the emitter, and used to obtain the ground position of the emitter from a database. The emitter’s ground position can then be used to determine the drone’s position accurately. *See* EX1010, ¶[0056]; *supra* at 37-38.

The ability to perform such emitter-signal-based location determination would be reduced significantly, if not disabled entirely, in the combination of Taveira and Qi (the “Taveira-Qi combination”) that Petitioner proposes. *See DePuy*, 567 F. 3d at 1326. This is because, if an RF emitter updates its SSID / MAC address (hereinafter, “emitter ID,” for brevity), that emitter ID would not be found in the database of RF emitter characteristics, unless the updated emitter ID is also associated with that RF emitter’s location in the database. If the emitter ID is changed periodically, several such emitter IDs would need to be added to the

database and associated with the emitter's location, before a drone receives an RF signal from the emitter.

In addition, the Taveira-Qi combination creates several significant design problem that would strongly discourage a POSITA from processing with the combination. The first significant design problem with the Taveira-Qi combination is that Qi does not describe whether the periodic update of the SSID is limited, i.e., cycling through only a fixed set of SSIDs, or not so limited, where a new SSID is provided at each update. *See* EX1013, ¶¶[0105]-[0107], [0128]-[0130], [0168]-[0169], [0173]-[0175], [0181], [0211]-[0213]. In the latter case, a periodic update of emitter IDs in Petitioner's proposed combination would result in an infinite sequence of emitter IDs, making their storage in the database infeasible, unless a methodology is employed to purge certain previously used emitter IDs.

The second significant design problem with the Taveira-Qi combination is that Taveira and Qi do not teach or suggest updating / managing a database of RF emitter characteristics such that the location of an RF emitter is associated with not one but several different emitter IDs (SSIDs or MAC addresses), potentially requiring purging of old emitter IDs. *See* Pet. at 60-64, EX1003, ¶¶172-187; *see generally*, EX1010; EX1013. Additionally, a POSITA would have been discouraged to modify a database in this manner because, when several emitter IDs are associated with the stored location of an emitter, the search for the location can

become complex and may take longer. This is not desirable for determining the location of a drone accurately, in a short time, because a drone typically moves rapidly. *See* EX1001, 10:66-11:4 (indicating fast drone movement).

The third significant design problem with the Taveira-Qi combination is that it requires a third-party entity to provide from time-to-time, e.g., periodically, certain data, e.g., service name keys, to **both** Taveira's RF emitter and drone, which the RF emitter and drone would use to generate periodically changing yet matching SSIDs. This third-party entity would have to provide this data at a potentially massive scale to potentially hundreds if not thousands of managed drones, hundreds or thousands of times per second to each drone. The above-discussed daunting but essential modifications of Taveira are rather complex, and outside the scope of the knowledge of a POSITA. Petitioner and Dr. Chowdhary do not discuss these modifications and how a POSITA would make them. *See* Pet. at 60-64; EX1003, ¶¶172-187. Thus, contrary to Petitioner's argument, that its proposed modification would have been "merely combining prior art elements ... [by] known methods ... to yield predictable results," *id.* at 61, Petitioner's proposed modification is significantly complex, undesirable, and impractical, if not infeasible for at least the three significant design problems with the combination that are noted above.

By not addressing the aforementioned design problems, Petitioner, Dr. Chowdhary, Taveira, and Qi teach or suggest a combination that “would produce an inoperative result.” *DePuy*, 567 F. 3d at 1326; *see also*, *Pet.* at 60-64, EX1003, ¶¶172-187; *see generally*, EX1010; EX1013.

For the foregoing reasons, a POSITA would not combine Taveira and Qi, along with Gong. Notwithstanding the lack of motivation to combine, the Taveira-Wang-Gong combination fails to teach or suggest all of the limitations of Claim 21, as discussed below.

2. The Taveira-Qi-Gong Combination Does Not Teach or Suggest “a Secure Identifier” Recited in Claim 21

Taveira’s SSID, that is “periodically changed via updating (as opposed to being kept constant) as taught by Qi,” *see* *Pet.* at 62-64, does not teach or suggest “a secure identifier,” as discussed below. As a threshold matter, a POSITA would not combine Taveira and Qi because doing so would make Taveira’s SSID unsuitable for its intended and stated purpose of location determination. *See supra* § V.C.1.

In addition, Qi’s SSID does not change “predictably” as required by a proper interpretation of “a secure identifier.” *See id.* This is because, Qi describes that a “‘Service Provider’ of a service may be configured to generate a Service name key (‘service-name-key’),” and “may distribute the service name key to devices 102

and/or 140, for example, at service registration time, or at any other time, e.g., as part of any update,” or “devices 102 and/or 140 may retrieve and/or “pull” the Service name key from the “Service Provider”, e.g., periodically, for example, as part of an update procedure.” EX1013, ¶¶[0105]-[0107]; *see id.* ¶¶[0128], [0130], [0168], [0173], [0175]-[0179] (describing that sending and receiving devices may obtain updated service name keys from a Service Provider). The “SSID processor 129” of a sending device “may update the SSID based on the update of the service name key.” *See id.*, ¶[0169], FIG. 1. Without receiving certain data, e.g., the service name keys, the sending and receiving devices cannot determine and generate a sequence of corresponding SSIDs. As such, the updated SSIDs in the proposed combination do not amount to a secure identifier that changes “predictably” as required by a proper interpretation of “a secure identifier.” *See supra* § III.

Petitioner repeats its argument from Ground 2, that the encoded identifying information in Taveira’s heart beat signals teaches a secure identifier. *See Pet.* at 64. This argument is incorrect as discussed above for Ground 2. *See supra* 47-49. Petitioner does not contend in the proposed combination that Gong teaches or suggests “a secure identifier,” *See Pet.* at 53-55, 60-64.

Thus, in summary, Taveira, Qi, and Gong, individually or in combinations as proposed, do not teach or suggest “a secure identifier,” and thus fail to teach all of

the limitations of Claim 21. Accordingly, the Taveira-Qi-Gong combination does not render Claim 21 obvious.

D. Ground 4

1. A POSITA Would Not Combine Gong and Wang-II

A POSITA would not combine Gong and Wang-II because, *inter alia*, this combination (the “Gong-Wang-II combination”) does not provide a reasonable expectation of achieving the claimed invention. *Intelligent Bio-Systems*, 821 F. 3d at 1367; *Personal Web Technologies*, 848 F. 3d at 993-94; *Belden*, 805 F.3d at 1073.

The Ground 4 combination also lacks the “secure identifier” of claim 21. Petitioner argues that “Gong does not provide detail regarding ... components [for] wireless communications,” and hence, would combine Wang-II with Gong to “fill[] in the gaps left by Gong” “to yield predictable result[]” of “two-way wireless communication.” Pet. at 64-66. The “two-way communication” of Claim 21 also requires, however, “a secure identifier” that Gong and Wang-II do not disclose, as discussed below. *See infra* § VI.D.2. thus, the Gong-Wang-II combination does not provide a reasonable expectation of achieving the claimed invention.

Intelligent Bio-Systems, 821 F. 3d at 1367; *Personal Web Technologies*, 848 F. 3d at 993-94; *Belden*, 805 F.3d at 1073.

Therefore, a POSITA would not combine Gong and Wang-II.

Notwithstanding the lack of motivation to combine, the Gong-Wang-II combination fails to teach or suggest all of the limitations of Claim 21, as discussed below.

2. The Gong-Wang-II Combination Does Not Teach or Suggest a “Secure Identifier”

In Gong, a “UAV identifier may be broadcast[] when a communication between [a] UAV and [an] air control system may be encrypted or authenticated,” and that UAV identifier may be encrypted. EX1012, ¶[0271]; see Pet. at 74. Gong also states that “A UAV can communicate directly with ... one or more geo-fencing devices of an air control system,” EX1012, ¶[0315]. A “geo-fencing device” can detect a UAV and may be “portable.” *Id.*, ¶¶[0542], [0593]. Thus, Gong appears to disclose transmitting an encrypted UAV identifier to a detection system such as a geo-fencing device. Petitioner alleges that the encrypted UAV identifier teaches the claimed “secure identifier.” See Pet. at 74.

This argument is erroneous because, as discussed above, encrypting an identifier is neither necessary nor sufficient to provide a “secure identifier.” See *supra* at 9-11. Rather, a “secure identifier” is properly understood as an identifier “that changes predictably to avoid spoofing and/or cloning of UAV transmissions across [a] connection” between a UAV and a detection system. See *supra* § III. An

encrypted UAV identifier of the Gong-Wang-II combination does not change predictably.

Moreover, “a secure identifier” is also “an identifier that identifies a connection for exchanging information between a UAV and a remote portable detection system.” *See supra* § III. The encrypted UAV identifier of the Gong-Wang-II combination may identify a UAV. The UAV identifier does not identify a connection between a UAV and a detection system. Neither Gong nor Wang-II teaches or suggests an identifier that can identify a connection and that can change predictably. *See generally*, EX1012; EX1014. Petitioner and Dr. Chowdhary do not contend that the Gong-Wang-II combination teaches or suggests such an identifier. *See* Pet. at 64-78; EX1003, ¶¶188-212. Accordingly, the Gong-Wang-II combination does not teach or suggest the claimed “secure identifier.”

In summary, Gong and Wang-II, individually or in combinations as proposed, do not teach or suggest “a secure identifier,” and thus fail to teach all of the limitations of Claim 21. Accordingly, the Gong-Wang-II combination does not render Claim 21 obvious.

Claim 21 is patentable because none of Grounds 1-4 teaches or suggests each and every limitation of Claim 21.

VI. CONCLUSION

For the foregoing reasons, Patent Owner submits that Petition does not demonstrate a reasonable likelihood of showing that Claim 21 is unpatentable. Therefore, Patent Owner respectfully request that the Board deny institution of this IPR.

Dated: July 11, 2025

Respectfully submitted,

/Suhrid Wadekar/

Suhrid Wadekar
Registration No. 65,595
Counsel for Patent Owner
Airspace Systems, Inc.

Certificate of Compliance with Word Count

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Patent Owner Preliminary Response complies with the type-volume limits of 37 C.F.R. § 42.24(b)(1) because it contains 12,930 words (excluding the parts of this Patent Owner's Preliminary Response that are exempted by 37 C.F.R. § 42.24(a)), according to the word processing system used to prepare this Patent Owner's Preliminary Response.

Dated: July 11, 2025

Respectfully submitted,

/Suhrid Wadekar/

Suhrid Wadekar
Registration No. 65,595
Counsel for Patent Owner
Airspace Systems, Inc.

Certificate of Service

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing PATENT OWNER’S PRELIMINARY RESPONSE was served via email on July 11, 2025 (per counsel’s consent) to lead and backup counsel of record for Petitioners as follows:

Chad C. Walters, Baker Botts L.L.P

chad.walters@bakerbotts.com

Harrison Rich

harrison.rich@bakerbotts.com

Joseph Andrew Grado

andrew.grado@bakerbotts.com

Ellyar Barazesh

ellyar.barazesh@bakerbotts.com

DLAxonDedroneIPRs@bakerbotts.com

Dated: July 11, 2025

Respectfully submitted,

/Suhrid Wadekar/

Suhrid Wadekar
Registration No. 65,595
Counsel for Patent Owner
Airspace Systems, Inc.