CRAIG H. MISSAKIAN (CABN 125202)
United States Attorney

JEFF MITCHELL (CABN 236225)
Chief, Criminal Division

NICHOLAS M. PARKER (CABN 297860)
ERIC CHENG (CABN 274118)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7368
nicholas.parker3@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ABDULRAHMAN ALFOZAN, Defendant.	CASE NO. 3:26-MJ-71329 MAG **MEMORANDUM IN SUPPORT OF UNITED STATES' MOTION FOR DETENTION** Hearing Date: October 19, 2026 Hearing Time: 11:00 a.m. Courtroom: A (15th Floor) Judge Hon. Alex G. Tse

I. INTRODUCTION

The defendant, Abdulrahman Alfozan, a now-former engineer at OpenAI, is charged with concealing a sophisticated recording device in an executive OpenAI conference room in an effort to secretly and unlawfully record the oral communications of the persons meeting in that room, in violation of 18 U.S.C. § 2511(1)(b). The government submits this memorandum in support of its motion that the defendant, a Saudi national with considerable resources and ties to Saudi Arabia, be detained pending trial. As alleged in detail in the Complaint (Dkt. 1), and as set forth herein, the defendant was mere days away from leaving the United States for Saudi Arabia when he was arrested.

The defendant is a Saudi citizen who had been pursuing opportunities in Saudi Arabia before he was arrested. He had intended to fly from San Francisco to Riyadh (via Istanbul) with his wife and son on a one-way ticket on October 12, 2026. Having been arrested by the FBI three days prior, the defendant did not make that flight. His wife and son, however, immediately left the United States without him. Rather than wait until the October 12 flight as booked, they initially planned to fly to Jeddah, Saudi Arabia, on October 11 on a one-way ticket booked and paid for by the Saudi government. That flight was canceled, however, when a member of the Saudi military booked and paid for yet another one-way ticket for the defendant's wife and son, this one business class to Doha, Qatar, on October 10, 2026. They did make that flight, departing San Francisco about 36 hours after the defendant was arrested. The day before she left the United States, the defendant's wife told the FBI agents who interviewed her that her U.S. visa was expiring and that she and her son were *permanently* moving back to Saudi Arabia—and that her husband, the defendant, eventually intended to do the same.

The defendant no longer has a job in the United States; OpenAI fired him after his arrest. He has never before faced criminal prosecution. His wife and young son have already departed the United States and now reside in Saudi Arabia, with no designs on returning to the United States. So, too, do both of his parents and all (or all but one) of his siblings. He has ample resources—including his significant compensation from a decade of high-tech employment in the Bay Area and at least two bank accounts in Saudi Arabia—and what appears to be considerable support from a foreign government that has (i) no extradition treaty with the United States; (ii) limitless resources; and (iii) the ability to provide extraordinary travel assistance, including based on similar circumstances in this District.[1] Ultimately, the defendant has little incentive to remain in the United States to see this case through. To ensure his appearance in court and the safety of the community, the Court should order the defendant detained pending trial.

[1] For example, as alleged in the Complaint and Superseding Indictment charging violations of 18 U.S.C. § 951 (Acting as an Agent of a Foreign Government) in *U.S. v. Ahmad Abouammo, et al.*, after Twitter confronted employee Ali Alzabarah in December 2015 about his access of internal Twitter user data and placed him on administrative leave from the company, numerous phone calls were immediately exchanged with a Saudi foreign official and the Saudi Arabian Consul General in Los Angeles to coordinate a next-day flight to Saudi Arabia, where Alzabarah became employed with the Misk Foundation. *See* Case No. 3:19-cr-00621-EMC (N.D. Cal.), Dkt. No. 1 ¶¶ 84-93 & , Dkt. No. 53 ¶ 26. The charges involving Alzabarah remain pending.

II. PROCEDURAL BACKGROUND

The defendant was charged by Complaint with using or endeavoring to use an electronic, mechanical, or other device to intercept oral communications, in violation of 18 U.S.C. § 2511(1)(b), on October 8, 2026. *See* Dkt. 1. He was arrested the next day and made his initial appearance in this Court on October 13, 2026. *See* Dkt. 5. The government moved for a detention hearing at that time, based on a "serious risk that [the defendant] will flee," 18 U.S.C. § 3142(f)(2)(A), and, upon agreement of the parties, the Court set a detention hearing for October 19, 2026. *See* Dkt. 5. The defendant has been in continuous federal custody since his arrest on October 9, 2026, and the government seeks his continued pretrial detention due to the serious risk of defendant's flight or nonappearance in these proceedings.

III. FACTUAL BACKGROUND

A. The Defendant's Conduct

The defendant is a Saudi national who at the time of his arrest resided in Millbrae, California, with his wife and their three-month-old baby. The defendant became a legal permanent resident (LPR) of the United States in September 2020 and has applied to become a naturalized U.S. citizen. His wife, on the other hand, was lawfully present in the United States on an F1 non-immigrant student visa, which recently expired. The defendant received technical degrees at MIT and UC Berkeley and has spent about a decade in the high-technology industry around the San Francisco Bay Area, joining OpenAI as an engineer in or around July 2025 with an annual base salary of $325,000 (later increased to $385,000) and a new hire equity grant of $2,200,000 in profit participation units.

According to information received from OpenAI, the defendant was scheduled to take two months of parental leave beginning in October 2026, and, as alleged in detail in the Complaint (Dkt. 1), he and his family were scheduled to fly on a one-way itinerary to Saudi Arabia on October 12, 2026. On or about September 28, 2026—about two weeks before their scheduled flight—the defendant inserted a surreptitious audio recording device into a USB port on the back of a television in an executive OpenAI conference room, where the device remained for at least multiple days. The defendant had modified the device to prevent data transfer between it and the television into which it was inserted. He had also encrypted the content stored on the device's microSD card and, in the days preceding installation of the device, used an AI chatbot account subscribed to his wife to research (among other things) how to "build a

continuous audio recorder" to "captur[e] microphone audio and save compressed WAV recordings to an SD card"; "improve audio and live listening"; "develop … speech-triggered recording"; "add browser access and controls," including "live listening"; and "encrypt the SD card" and "decrypt[] and recover[] recordings from the removed card." Dkt. 1 at ¶¶ 11–18.

So, too, did the defendant research in advance where precisely he should install his customized listening device. In the days and weeks before placing the device, the defendant (i) used an OpenAI productivity agent to ascertain which "meeting rooms" OpenAI "leadership and exec[utives]" used, and where they met with "external partners"; and (ii) spent considerable time near the conference room where he later installed the device. Dkt. 1 at ¶¶ 14–16. In fact, and as known to the defendant, the conference room in which the defendant installed the device is typically used for internal OpenAI leadership meetings and technical and product sessions, as well as external briefings with government officials and business counterparts. *See* Dkt. 1 at ¶ 9. Meetings in that room, which the defendant had no authority to participate in, frequently involve discussions of highly confidential technical, commercial, and strategic information, including proprietary research, as well as nonpublic information about OpenAI's technical progress and strategic decisions, capabilities, priorities, government engagements, and commercial relationships. *See* Dkt. 1 at ¶ 10.

For instance, in the days surrounding the time period that the device was installed, OpenAI executives met with government officials in that very room. Defendant's conduct could pose a danger to the national security of the United States.

B. The Defendant's Arrest and Relevant Post-Arrest Facts

The defendant was arrested on October 9, 2026—four days after OpenAI security personnel found and confiscated a second, similar recording device in a bag the defendant had left unattended in an OpenAI printer room[2] and three days before he was scheduled to fly from San Francisco to Riyadh (via Istanbul) on a one-way itinerary with his wife and young son. The defendant invoked his right to an attorney and did not speak with the arresting agents. His wife did, however, and she told them, among

[2] As described in the Complaint, the defendant reported his bag missing but, when he retrieved it from OpenAI's Lost and Found on October 6, 2026, he inquired about certain "stolen" items, including a credit card and cash, but not about the confiscated recording device.

other things, that she had seen her ChatGPT account open on her husband's laptop and that she and her son were moving back to Saudi Arabia permanently. She added that her husband planned to return to the United States to resume working at OpenAI after spending two months in Saudi Arabia but that he, too, intended at some point to move to Saudi Arabia permanently to live there with her and their son. The defendant's wife and son in fact flew from San Francisco to Doha, Qatar, on October 10, 2026—the day after the defendant was arrested—on a one-way, business-class ticket booked and paid for by a Saudi military official.

The government's investigation is ongoing and may result in additional serious charges. At this point, however, the government is aware of the following facts, among others, following a search of the defendant's residence and a preliminary review of his electronic devices, including his cellphone:

- The defendant's residence contained several electronic components similar to those in the customized devices the defendant installed in the OpenAI conference room and had in his missing bag.
- The defendant's iPhone contained photographs, dated between September 22–28, 2026, depicting, among other things, at least one additional concealed recording device as well as what appear to be the input/output panels on televisions and other electronic devices in various locations in OpenAI buildings, including another conference room where sensitive meetings frequently occurred.
- The defendant's cellphone included several relevant, recently modified notes, including:
  - A deleted note from September 2026 with links to various recording devices, including devices made by Seeed Studio, the manufacturer of the devices OpenAI found in its offices and the devices FBI agents found in the defendant's residence;
  - A note entitled "Riyadh tasks" (last modified September 13, 2026) that listed various action items, including finding an apartment and a job for the defendant's wife, as well as obtaining an ID and a Saudi passport for his son; and
  - A note entitled "OpenAI leave" (last modified October 7, 2026) that suggested the defendant was planning an "[e]arly … pick up" of the devices he had installed or intended to install and then extending his planned parental "leave to full."

- Throughout 2025 and 2026, the defendant was in frequent communication via WhatsApp with a member of the Saudi Royal Family, including as recently as October 5, 2026. Among other things, the individual told the defendant that an artificial intelligence initiative was being launched in Saudi Arabia and wanted the defendant to join it. In May 2026, the individual told the defendant, "Saudi needs you more then [*sic*] the US!" to which the defendant responded "100," indicating he agreed. The individual repeatedly tried to recruit the defendant and asked when he planned to leave OpenAI. At the time, the defendant said he wouldn't leave until his stock vested.
- The defendant was pursuing other opportunities in Saudi Arabia, including participating in the Misk Foundation's "2030 Leaders" program,[3] which would have required his in-person participation in Riyadh. The defendant visited the "2030 Leaders" program application portal on or about July 7, 2026, and had applied by July 18, 2026, when he received an email with the subject line: "You made it to stage 2 of the 2030 Leaders Program Cohort 8." The defendant's browsing history further showed that on August 7, 2026, he had accessed a page displaying "Confirmed: 2030 Leaders Program Cohort 8 Online Assessment on Monday, August 10, 2026." And on September 4, 2026, he accessed a page displaying "Update Regarding Your Application to 2030 Leaders Program Cohort 8."
- The defendant's browsing history further showed that he accessed a folder called "Saudi Gov Docs" on October 4, 2026, and the defendant used an OpenAI productivity agent to inquire about multiple Saudi-related business and government-related engagements from the Saudi Ministry Communication and Information Technology (MCIT) between July 6, 2026, and September 21, 2026. To that end, he issued the following prompts, among others:
    - July 6: "who from openai could be suitable to attend a high level informal meeting with ministers in Saudi arabia? list 10 people and why each. ideally high levels."

[3] According to its website, the Mohammed bin Salman (Misk) Foundation's "2030 Leaders" program "is an exclusive world-class leadership development program that will transform exceptional senior Saudi leaders to change history and achieve our one common goal - realizing Saudi's Vision." *See* https://misk.org.sa/leaders2030/#about (last visited Oct. 17, 2026). The program is open only to Saudi nationals 45 or younger who are "[p]roficient in spoken and written English." *Id.*

- September 5: "list planned openai visits to Saudi this year. search notion, slack, docs."
- September 7: "if there's a meeting for "HUMAIN x MCIT @OpenAI" meeting, who will likly [*sic*] attend? list 15 names."
- September 8: "find info about upcoming Saudi MCIT visit on Sept 9."
- September 21: "look at email from MCIT - and search for related context internally - slack, notion, ask, docs,.... and get me up to date."

IV. LEGAL STANDARD

Under the Bail Reform Act of 1984, the Court must detain a defendant before trial without bail where "the judicial officer finds that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person in the community." 18 U.S.C. § 3142(e)(1). Detention is appropriate where a defendant is either a danger to the community or a flight risk; the government need not prove that both factors are present. *See United States v. Motamedi*, 767 F.2d 1403, 1406 (9th Cir. 1985). A finding that a defendant is a danger to the community must be supported by clear and convincing evidence, but a finding that a defendant is a flight risk need only be supported by a preponderance of the evidence. *See id.*; *United States v. Aitken*, 898 F.2d 104, 107 (9th Cir. 1990); *United States v. Winsor*, 785 F.2d 755, 757 (9th Cir. 1986). To support pretrial detention based on risk of flight, the government "must demonstrate that it is more likely than not that there is a serious *risk* that the defendant will flee, not that it is more likely than not that the defendant *will* flee." *United States v. Figueroa-Alvarez*, 681 F. Supp. 3d 1131, 1138-39 (D. Idaho 2023).

The Court must consider the following factors in its detention analysis: (1) the nature and circumstances of the offense charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant, including among other things the defendant's family and community ties; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. *See* 18 U.S.C. § 3142(g); *Winsor*, 785 F.2d at 757.

Evidentiary rules do not apply at detention hearings, and the government is entitled to present evidence by way of proffer, among other means. *See* 18 U.S.C. § 3142(f)(2); *Reem v. Hennessy*, 2018 WL 1258137, at *2 (N.D. Cal. Mar. 12, 2018); *see also United States v. LaFontaine*, 210 F.3d 125, 130-

31 (2d Cir. 2000) (holding that the government is entitled to proceed by proffer in detention hearings). In the pretrial context, few detention hearings involve live testimony or cross-examination. Most proceed by proffer. *LaFontaine*, 210 F.3d at 131. This is because bail hearings are "typically informal affairs, not substitutes for trial or discovery." *Id*. (internal quotation marks omitted).

In this case, each of the relevant statutory factors in the detention analysis underscore that the defendant presents both an ongoing danger to the community and a serious risk of flight if released on bond, no matter what conditions are in place.

V. ARGUMENT

A. Nature and Circumstances of the Offense Charged

The first factor in the Court's detention analysis contemplates consideration of not only the specific acts and charges alleged, but also the potential penalty that may be imposed if the person is convicted. *See, e.g.*, *United States v. Hir*, 517 F.3d 1081, 1086 (9th Cir. 2008); *United States v. Townsend*, 897 F.2d 989, 995 (9th Cir. 1990).

Here, the nature and circumstances of the offense are indisputably serious. The defendant went to significant lengths to create customized, encrypted recording devices to secretly record highly sensitive meetings involving senior OpenAI personnel and executives, high-level business counterparts, and government officials, all while communicating with individuals of significance in Saudi Arabia and pursuing opportunities in—and making plans to travel to—Saudi Arabia. These facts put our national security at risk and heighten the risk the defendant will flee.

This is an ongoing investigation that may yet result in more serious charges. Regardless, however, the five-year prison sentence the defendant faces if he is convicted on the charged offense—a statutory maximum sentence that, to be sure, is less significant than others in federal criminal law, but that nevertheless represents a significant custodial term for someone who, like the defendant, has never before been prosecuted, let alone incarcerated—provides yet another incentive for the defendant to flee the United States rather than see this case to its conclusion. *See Townsend*, 897 F.2d at 995; *see also United States v. Cisneros*, 328 F.3d 610, 618 (10th Cir. 2003) (holding defendant was a flight risk because her knowledge of the seriousness of the charges against her gave her a strong incentive to abscond). This factor weighs heavily in favor of detention.

B. Weight of the Evidence Against the Defendant

The weight of the evidence against the defendant may be the least important factor in the Court's detention analysis, *see Townsend*, 897 F.2d at 994; *Winsor*, 785 F.2d at 757, but it is nevertheless a relevant consideration, particularly as it relates to the defendant's incentive to evade prosecution. *See Motamedi*, 767 F.2d at 1408.

Here, the weight of the evidence against the defendant is considerable. As described herein and in the Complaint (Dkt. 1), the defendant researched how to build a surreptitious audio recording device; how to modify it to prevent unwanted data transfer, develop speech-triggered recording, improve live-listening capabilities, save compressed WAV files to a built-in microSD card, and add remote-access controls; and how to encrypt and decrypt it so only he could access its contents. So, too, did the defendant research where precisely he should install his customized listening device, focusing on OpenAI meeting rooms that would involve highly sensitive and confidential discussions between and among OpenAI executives, government officials, and business counterparts regarding, among other things, commercial relationships and strategic decision making, as well as nonpublic information about OpenAI's proprietary technologies and capabilities, and its commercial priorities and government engagements. He then installed his customized listening device in an executive conference room at OpenAI and was caught on camera looking for that device—which OpenAI security personnel had removed a few days prior—on October 5, 2026, about 20 minutes before he reported to OpenAI that he had misplaced a bag that contained another, similar recording device. When he retrieved his bag from Lost and Found the next day, the defendant noted certain missing items but conspicuously omitted the recording device. The defendant also had in his residence various electronic component parts similar to those found in the customized devices he installed and possessed at OpenAI, and FBI agents found photographs on the defendant's cellphone that suggested he had done reconnaissance at OpenAI to determine where he might install additional devices.

Where, as here, the evidence of the defendant's guilt is strong, there is "a considerable incentive to flee." *United States v. Millan*, 4 F.3d 1038, 1046 (2d Cir. 1993); *see also Motamedi*, 767 F.2d at 1408 (9th Cir. 1985); *United States v. Palmer-Contreras*, 835 F.2d 15, 18 (1st Cir. 1987) (where "the evidence

against defendants is strong, the incentive for relocation is increased"). This factor, too, militates in favor of detention.

C. History and Characteristics of the Defendant

The defendant is a Saudi national who arrived in the United States in 2009, went to college and graduate school here, and became an LPR in September 2020. He has had high-paying jobs at various technology companies in the San Francisco Bay Area, but he no longer has a job and now that his wife and son have returned to Saudi Arabia, he has significant ties to that country and few ties to the United States. Indeed, his parents and all (or all but one) of his siblings reside in Saudi Arabia, as well, as do many of the defendant's friends and professional acquaintances, as reflected in the list of contacts in his phone. He regularly travels to Saudi Arabia (among other places) for both business and pleasure. He has considerable resources in U.S. accounts and an unknown sum in at least two Saudi bank accounts. Although FBI agents seized the defendant's Saudi passport when they arrested him, there is nothing to stop the defendant, if he is released, from obtaining any necessary travel documents and fleeing the United States—with or without the help of a foreign government that has previously assisted its citizens depart the United States under similar circumstances. The defendant presents a serious risk of flight. The Court should detain him pending trial to assure his appearance.

D. Nature and Seriousness of the Danger to the Community

In evaluating the nature and seriousness of the danger a defendant poses to the community, the Court may consider, among other things, whether the charged offense carries severe penalties and whether it required intelligence, planning, capital, facility in deception, international communications, or international motives. *See Townsend*, 897 F.2d at 996.[4] Here, the defendant leveraged his skills as a highly-educated engineer to create sophisticated recording devices that—the evidence strongly suggests—he intended to bring with him to Saudi Arabia. Whether the defendant wanted to record OpenAI meetings to enrich himself by enhancing his own business prospects, or to provide aid a foreign

[4] Other factors listed in *Townsend* are inapplicable here. *See* 897 F.2d at 996 (listing factors such as the defendant's criminal history and prior performance on court-imposed supervision; whether the defendant illegally possessed firearms or large quantities of prohibited drugs; and, whether the defendant was on probation, parole, supervised release, or subject to conditions of pretrial release at the time he committed the charged offense).

government, or both, his conduct is criminal and it presents a danger to innovation in the Silicon Valley and a concern for the national security of the United States.

VI. REQUEST FOR STAY OF RELEASE ORDER

If the Court finds that release is appropriate, the government respectfully requests that the Court exercise its inherent power to control its docket by staying any release order to give the government an opportunity to appeal to the district judge. *See* Fed. R. Crim. P. 47 (governing criminal motion practice generally); *CMAX, Inc. v. Hall*, 300 F.2d 265, 268 (9th Cir. 1962) (discussing courts' inherent authority). Here, a stay of any release order would be necessary to ensure meaningful review by the district judge. Without such a stay, the defendant would be released soon after the detention hearing, depriving the government of an opportunity for appellate review.

VII. CONCLUSION

The defendant presents an ongoing danger to the community and a serious risk of flight that no set of release conditions can reasonably mitigate. The defendant has every incentive to flee. He faces prison time in the United States. His wife and son are now in Saudi Arabia and have no plans to return. He has the resources to flee. He has the connections needed not only to flee, but to build a new life in Saudi Arabia. The Court should order the defendant detained pending trial.

DATED: October 18, 2026

Respectfully submitted,

CRAIG H. MISSAKIAN
United States Attorney

/s/ Nicholas M. Parker
NICHOLAS M. PARKER
ERIC CHENG
Assistant United States Attorneys