



PRESS RELEASE

Saudi National Arrested for Installing Surreptitious Audio Recording Device at OpenAI

Tuesday, October 13, 2026

For Immediate Release

Office of Public Affairs

An employee of OpenAI has been arrested for and charged with using or endeavoring to use an electronic, mechanical, or other device to intercept oral communications. Abdulrahman Alfozan, 35, a national of the Kingdom of Saudi Arabia, was arrested on Oct. 9, and made his initial appearance in federal court today.

“This serious situation underscores why winning the global super intelligence race is a national security prerogative — and why President Trump’s leadership in creating the Super Intelligence Force is so important,” said Director of National Intelligence Jay Clayton. “I thank Director Patel and our FBI partners for their diligence and swift action. The intelligence community remains committed to safeguarding America’s cutting-edge intellectual property from foreign threats.”

“According to the complaint unsealed today, Abdulrahman Alfozan allegedly concealed a covert recording device inside his employer’s executive conference room to secretly capture sensitive communications about the company’s super intelligence technology,” said FBI Director Kash Patel. “Protecting American SI innovation is essential to safeguarding our nation’s economic strength and national security, and the FBI views that mission as one of our highest counterintelligence priorities. Thank you to Director of National Intelligence Jay Clayton and our law enforcement partners for their support — and we will continue working closely with our partners across the U.S. government and private sector to keep American businesses and citizens safe and to ensure our country maintains its competitive edge.”

“The Bay Area and Silicon Valley lead the world in developing tomorrow’s technology, and our Office will continue to stand at the forefront of protecting that American innovation,” said U.S. Attorney Craig H. Missakian for the Northern District of California. “For us it is a matter of national security. This arrest highlights our relentless efforts in partnership with the FBI to identify and prosecute those who seek to steal our technology, as alleged in the complaint.”

According to the complaint, Alfozan had been employed as an engineer by OpenAI since July 2025. On or about Sept. 30, OpenAI personnel discovered a surreptitious audio recording device (Recording Device 1) inserted into a USB port on the back of a television in an executive conference room inside one of their buildings in San Francisco. OpenAI determined that the device, which had been concealed in toilet paper, was installed on or about Sept. 28, and that its contents were encrypted.

Figure 1



Figure 2 (Recording Device 1)



CREDIT: U.S. v. Abdulrahman Alfozan, 3:26-mj-71329

Closed-circuit television (CCTV) footage inside OpenAI's office showed that Alfozan appeared near the executive conference room on multiple dates prior to the device's discovery, although he had no authority to access or to participate in meetings occurring in the executive conference room. According to the complaint, meetings in the executive conference room where Recording Device 1 was discovered frequently involved discussions of highly confidential technical, commercial, and strategic information, including proprietary research, product plans, and business-development opportunities, as well as nonpublic information about Open AI's technical progress and strategic decisions, capabilities, priorities, government engagements, and commercial relationships.

According to the complaint, prior to Sept. 28, Alfozan used a productivity tool to make multiple inquiries about Open AI's building addresses, meeting rooms, meeting-room capacities and calendars, "leadership and exec" locations, and external partner meetings. Moreover, a chatbot account associated with Alfozan's spouse (which shared multiple identifiers and attributes with Alfozan's own chatbot account) submitted prompts between Sept. 24 and Sept. 30 related to building, customizing, installing, audio recording, testing, obfuscating, and remote accessing a device, including inquiries about "build[ing] a continuous audio recorder," "customiz[ing] Wi-Fi . . . connectivity," "improv[ing] audio and live listening," and "encrypt[ing] the SD card," among other things. The same chatbot account also submitted prompts specifically related to Recording Device 1, including its custom header and unique MAC address, between Sept. 27 and Sept. 28.

The complaint further alleges that on Oct. 5, Alfozan entered the executive conference room and appeared to look behind the television into which Recording Device 1 had been inserted, as captured below:



Image of Alfozan

Finally, the complaint alleges that, also on or about Oct. 5, Alfozan left a bag unattended in a different room in an OpenAI building. OpenAI security personnel found and opened Alfozan's bag, inside which they discovered — among other things, including Alfozan's wallet and ID — another recording device (Recording Device 2) similar to Recording Device 1.

If convicted, Alfozan faces a maximum penalty of 5 years in prison and a \$250,000 fine, followed by 3 years of supervised release.

The FBI is investigating the case.

Assistant U.S. Attorney Nicolas Parker for the Northern District of California is prosecuting the case with valuable assistance from Trial Attorney Kate Tagert of the National Security Division's Counterintelligence and Export Control Section.

This prosecution is in support of National Security Presidential Memorandum 11 ([NSPM-11](#)) designed to support American superiority in super intelligence technology.

Updated October 13, 2026

Topic

NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI)

Press Release Number: 26-1173

Related Content



PRESS RELEASE

Bosnian National Sentenced for Violating International Sanctions Against North Korea

October 14, 2026

PRESS RELEASE

Leader of Global Violent Extremist Network ‘764’ Pleads Guilty to Conspiracy to Sexually Exploit Minors

October 9, 2026

PRESS RELEASE

Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated and Used by China-State Sponsored Hackers

October 8, 2026