OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN DEPTH

17 NOVEMBER 2020 IA-47794-21

*COUNTERINTELLIGENCE*

# *(U//FOUO)* ADMINISTRATIVE REVISION: Chinese Security Company Poses Multiple Challenges

*(U//FOUO)* ***Scope Note:*** *This Intelligence In Depth (IID) addresses requests to better understand the continual risks and threats posed by Nuctech, a foreign security company that provides screening and detection systems to state and local governments. This IID advances the understanding of the DHS Intelligence Enterprise (DHS IE) and the broader US Government concerning the company's relationship with the Chinese Government, alleged illegal business practices, and concerns regarding both the security and data privacy of its screening and detection systems. The information cutoff date for this IID is 18 August 2020.*

## *(U)* Key Judgments

- *(U//FOUO) Key Judgment 1:* **We assess that Nuctech very likely has a close and enduring relationship with the Chinese Government to advance Nuctech's business interests and develop screening and detection systems on behalf of the Chinese Government**.
- *(U//FOUO) Key Judgment 2:* **We assess that Nuctech has engaged, and will likely continue to engage, in illegal business practices that include corruption, bribery, and product dumping to gain an unfair market advantage**.
- *(U//FOUO) Key Judgment 3:* **We assess that Nuctech's screening and detection systems likely have deficiencies in detection capabilities, which may create opportunities for exploitation by the Chinese Government.**
- *(U//FOUO) Key Judgment 4:* **We assess that Nuctech's COVID-19-related screening and detection systems likely present concerns about individual privacy based on their ability to leverage artificial intelligence and machine learning, specifically facial recognition technology**.

*(U)* Prepared by the Counterintelligence Mission Center. Coordinated within the DHS Intelligence Enterprise (I&A Field Operations Division (FOD), CISA, CWMD, TSA) and FBI. For questions, contact DHS-SPS-RFI@hq.dhs.gov.

### *(U)* Background on Nuctech

*(U//FOUO) Nuctech is a large Chinese security company founded in 1997 as a high-tech spin off of Tsinghua University and formerly led by Hu Haifeng, son of former Chinese president Hu Jintao, according to open source reporting. Nuctech primarily specializes in providing security screening and detection systems such as x-ray machines and airport scanners and presently continues to maintain ties with Chinese State Owned Enterprises (SOEs) such as the China National Nuclear Corporation (CNNC), which manages China's civilian and military nuclear programs.*

*(U//FOUO) Since at least 2016, Nuctech has demonstrated a persistent interest in expanding its business with US federal, state, and local governments – including DHS – according to open source news reporting. While Nuctech has previously sought for its systems to be used by TSA in airports, these efforts have since been largely stalled. Currently, only two Nuctech systems are grandfathered in the Air Cargo Screening Technology List and these systems are set to expire for consideration by TSA after 2020. Nuctech now primarily sells systems for use by state and local governments in applications such as prisons and ports of entry (POEs) with mixed results. In one such instance, a $2.4 million contract with a US POE was cancelled after Nuctech's systems were found to be defective. Beyond prisons and POEs, Nuctech has recently capitalized on the COVID-19 pandemic by offering systems to screen for abnormal temperatures to detect the presence of COVID-19.*

## *(U)* Nuctech's Relationship with the Chinese Government

*(U//FOUO)* **We assess that Nuctech very likely has a close and enduring relationship with the Chinese Government to advance Nuctech's business interests and develop screening and detection systems on behalf of the Chinese Government.** We have medium confidence in this assessment, as it relies on reporting that indicates Nuctech has conducted an operation with the Chinese Government, family ties exist between Nuctech's leadership and the Chinese Government, and Nuctech's former CEO moved to a position within a Communist Party Committee. Chinese national security laws passed in 2014, 2015, and 2017 can be used by the Chinese Government to compel Chinese businesses to cooperate and assist in matters of intelligence and national security.

- *(U//FOUO)* A Nuctech sales manager was discovered staging a "honey trap" operation in Taiwan in 2016, likely in concert with the Chinese Government, according to reputable Taiwanese press reporting.[a]
- *(U//FOUO)* Nuctech and Tsinghua University jointly built the Chinese National Engineering Laboratory for Dangerous Articles and Explosives Detection Technologies in 2017. This project was developed on behalf of the Chinese Ministry of Public Security to provide "fast and accurate detection of hazardous and explosive substances," according to reputable Western press reporting.

[a] (U) A honey trap is the practice of using romantic or sexual relationships to gain information or resources required by a group or individual.

- *(U//FOUO)* Nuctech was accused by its main European competitor in 2009 of off-loading its research and development costs onto the Chinese Government by using its connections to the Chinese Government to gain an unfair advantage, according to reputable Western press reporting.

- *(U//FOUO)* Nuctech's former parent entity, Tsinghua University, appears to have undertaken Chinese Government tasking to research and develop security screening technologies pursuant to a technological research program, according to a documentary published in 2018.

- *(U//FOUO)* Nuctech's former CEO, Hu Haifeng, was appointed to party secretary at Tsinghua Holdings in 2008 and subsequently to head the Communist Party Committee in Xi'an, according to reputable press reporting. Hu Haifeng's departure from Nuctech and subsequent employment with the Communist Party Committee may be indicative of ongoing cooperation between Nuctech and the Chinese Government.

## *(U)* Nuctech's Business Practices

*(U//FOUO)* **We assess that Nuctech has engaged, and will continue to engage, in illegal business practices that include corruption, bribery, and product dumping to gain an unfair market advantage.** We have high confidence in this assessment, as it relies on a history of reporting suggesting that Nuctech takes advantage of the venality of local officials and close ties with the Chinese Government.

- *(U//FOUO)* In February 2020, Taiwanese officials found the former head of Taiwan's aviation police bureau guilty of corruption during the procurement of Nuctech X-ray scanners, as additionally included in the prior key judgment. The investigation found that Nuctech had sent a female sales representative who engaged in a sexual relationship with the aviation security official to get information on the procurement process. The Taiwanese official also received financial kickbacks during the procurement.

- *(U//FOUO)* Namibia's Anti-Corruption Commission charged three people—one of whom was a Nuctech representative and one of whom was a Namibian civil servant—with fraud, corruption, and bribery in connection to a deal to purchase Nuctech scanners. According to an anti-CCP news outlet, the agreement to purchase scanners from Nuctech came after then-Chinese president Hu Jintao offered a loan to cover most of the costs as long as a Chinese company was awarded the contract. Approximately $12.8 million of the contract total of $55 million was directed to the consultancy the three men worked for. The three men were accused of bribery and price-fixing.

- *(U//FOUO)* A European academic research paper shows that Nuctech retaliated against an accusation by its main European competitor in 2009 by lodging a petition with the Chinese Ministry of Commerce (MOFCOM) for an anti-dumping investigation regarding the European competitor's products. MOFCOM responded by initiating an investigation into the European competitor and imposed an anti-dumping duty of 33.5 percent on the European competitor in 2011.

## *(U)* System Security Concerns

*(U//FOUO)* **We assess that Nuctech's screening and detection systems likely have deficiencies in detection capabilities, which may create opportunities for exploitation by the Chinese Government.** We have medium confidence in this assessment because while we lack specific information related to intent, media reports state that European Union (EU) officials have expressed concern regarding Nuctech systems, and additional media reporting indicates that at least one IP address associated with Nuctech's former parent entity has been implicated in at least three cyberattacks. While we do not have definitive evidence of backdoors or deficiencies in Nuctech systems, we suspect that if backdoors or deficiencies are present, remote access could be enabled to gain access of Nuctech systems and other networked infrastructure.

- *(U//FOUO)* Reputable Western press reports indicate that EU officials view Nuctech as a possible national security, counterintelligence (CI), and economic security risk, based on the alarming rate at which the security company continues to gain control over various strategic security infrastructure. Specifically, the concern is that Nuctech's equipment could potentially cause disruptions, or Nuctech's systems could transmit malicious code.
- *(U//FOUO)* Reputable Western press reports indicate that at least one IP address associated with Nuctech's former parent entity, Tsinghua University, has been implicated in multiple cyberattacks in the weeks before and after Alaska conducted a trade mission to China in August 2018.
- *(U//FOUO)* Reputable Taiwanese press reports indicate that Nuctech systems installed at multiple Taiwanese airports were initially defective and resulted in Taiwanese officials misreading screened luggage. In one notable instance, a live cat passed through Taiwanese airport security undetected and remained undiscovered until the luggage was scrutinized by South Korean officials.

## *(U)* COVID-19 Systems Development and Privacy Concerns

*(U//FOUO)* **We assess that Nuctech's COVID-19-related screening and detection systems likely present concerns about individual privacy based on their ability to leverage artificial intelligence and machine learning, specifically facial recognition technology.** We have medium confidence in this assessment, as it relies on a review from Nuctech's public website, which may overplay the capabilities of such devices.

- *(U//FOUO)* Nuctech's website indicates that the company began manufacturing, marketing, and selling two systems, the FeverBlock and TempCheck, in March 2020. Nuctech claims that these systems can screen more than 120 persons per minute from one to five meters. Nuctech's website additionally states that the deep learning algorithms installed on these devices can locate the face's position and alert if abnormal body temperatures are detected. While temperature detection capabilities do not present a privacy challenge by itself, the coupling of existing Nuctech systems with artificial intelligence and machine learning capabilities could potentially foster biometric collection opportunities, even if the person being scanned is wearing a mask. Such information could be gathered without notification or consent of individuals and used for

unknown purposes. Additionally, if the marriage of existing systems with advanced identification capabilities is used for illicit purposes, or if the systems are available to external parties beyond the receiving client's knowledge, this could raise additional privacy concerns.

*(U)* **Screenshot of Nuctech's COVID-19 screening and detection system, FeverBlock**


*(U)* **Screenshot of Nuctech's COVID-19 screening and detection system, FeverBlock**

## Source, Reference, and Dissemination Information

| | |
|---|---|
| **Source Summary Statement** | *(U//FOUO)* We have **medium confidence** in our assessment of the relationship between Nuctech and the Chinese Government because, while it relies on reporting that indicates coordination has taken place in support of an operation, proximity of associates, and family ties, these factors may be for other reasons. Additionally, we have **high confidence** in our assessment regarding Nuctech's unfair business practices, as it relies on a history of credible reporting relating to multiple instances of unfair and illegal business practices. We have **medium confidence** in our assessment that Nuctech's systems have deficiencies in detection capabilities due to a lack of specific information. While we have reporting on Nuctech's former parent entity, nothing directly implicates Nuctech. Our confidence level for this assessment would increase with the addition of reporting specifically mentioning Nuctech's systems being accessed beyond known deficiencies which may or may not pose security concerns. Finally, regarding our assessment that Nuctech's COVID-19 related systems present a threat to individual privacy, we have **medium confidence**. We lack a more detailed analysis of the capabilities of these systems and are reliant on information from Nuctech's website, which may exaggerate the capabilities of the devices. Deeper insight into these systems' technical capabilities would increase our confidence level. Our sourcing for this *IID* is a mix of DHS IE reporting as well as commercial and media-based open-source reporting. |
| **Releasable by Information Disclosure Official (RELIDO)** | *(U)* RELIDO is a permissive foreign disclosure and release marking used on information to indicate that the originator has authorized a Senior Foreign Disclosure and Release Authority (SFDRA) to make further sharing decisions for uncaveated intelligence material (intelligence with no restrictive dissemination controls) in accordance with the existing procedures, guidelines, and implementation guidance in this document. Second Party Integrees may access RELIDO information that is not CMI or SIGINT without a SFDRA review, including intelligence information created after 28 June 2010 - excluding SIGINT – which carries no foreign disclosure and release markings and hence is treated as if marked RELIDO. |
| **This product has been approved for release to the following countries** | *(U)* Antigua and Barbuda, Austria, Bahamas, Bangladesh, Barbados, Belize, Belgium, Bermuda, Brazil, Bulgaria, Chile, Columbia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominica, Dominican Republic, Egypt, El Salvador, Estonia, Finland, France, FVEY, Germany, Greece, Grenada, Guadeloupe, Guatemala, Haiti, Honduras, Hungary, Iceland, India, Ireland, Israel, Italy, Japan, Kazakhstan, Latvia, Lebanon, Lithuania, Luxembourg, Malta, Martinique, Mexico, Netherlands, Nicaragua, Norway, Oman, Panama, Philippines, Poland, Portugal, Qatar, Romania, Saudi Arabia, Singapore, Slovakia, Slovenia, South Korea, Spain, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Sweden, Switzerland, Taiwan, Trinidad and Tobago, Tunisia, Turks and Caicos, Uruguay, United Arab Emirates, and Vietnam |
| **Warning Notices & Handling Caveats** | *(U)* **Warning:** This document is the property of the Government of the United States. It is provided to international partners on the condition that it is for use solely by the intelligence and homeland security organizations of the receiving government and that it not be shared with any other government without the express permission of the Government of the United States.<br><br>*(U)* For comments or questions related to the contents or dissemination of this document, please contact the I&A Foreign Liaison Office at DHSI&AForeignLiaisonOffice@HQ.DHS.GOV. |