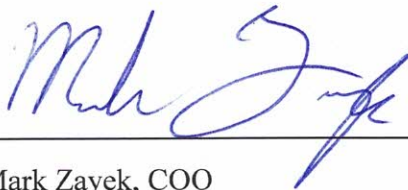


Mark Zayek
Chief Operating Officer
21481 Ferrero Parkway
City of Industry, Ca 91789 USA
T. (909) 598-5488

March 1, 2021
Francois Delisle
Approvisionnement Shadow Minister for Public Services and Procurement
Ottawa, Ontario, Canada K1A 0A6
T. (613) 943-5007

Dear Mr. Delisle,

On behalf of Astrophysics, we would like to submit a brief to the House of Common's Committee on Government Operations and Estimates in regards to the risks of Nuctech. We hope this brief clarifies the committees' current viewpoints on Nuctech.



Mark Zayek, COO



Global Security Threat: Nuctech

Chinese government agencies and state-funded businesses have been accused and implicated in economic espionage, intellectual property theft, personal data breaches, and cybersecurity attacks. Astrophysics, Inc. finds the unethical business practices of Nuctech and Chinese security technologies to be an eminent threat to both Canadian and broader western national security concerns. These concerns are due to Nuctech's relationship with the Chinese government and the People's Republic of China's (PRC) history of espionage, the inferior quality of their scanning equipment, and the total control of information the PRC exercises over companies operating within China along with Chinese companies abroad. Based on Nuctech's history of disreputable business dealings and their involvement in alleged Chinese espionage operations, the United States (U.S.) Department of Commerce placed Nuctech on the Bureau of Industry and Security (BIS) Entity List for specific scrutiny and licensing requirements. The Federal Bureau of Investigation (FBI) has expressed grave concerns over broader information security within systems using Chinese technology, and general interest into unforeseen future developments that could negatively impact the security of western nations as Chinese influence grows worldwide.

Connections to the Chinese Government

Nuctech is a state-owned company with multiple ties to various state-owned Chinese enterprises. The company was founded in 1997 as an offshoot of Tsinghua University¹, one of the C9 league of Chinese universities, a project started by the Chinese government in 1998 to expand university research.² Nuctech still maintains multiple ties to Tsinghua University; the company set up a joint research institute with the university in 2004 for "...co-investment and co-development, sharing intellectual property, and profits & risks."³ In addition, Nuctech and Tsinghua University co-constructed the *Chinese National Engineering Laboratory for Dangerous Articles and Explosives Detection Technologies* at the university, which launched on January 11, 2017.⁴

Nuctech was founded by Hu Haifeng, the son of former General Secretary of the Chinese Communist Party (CCP) Hu Jintao. Hu Haifeng served as chairman of Nuctech until 2008. In addition, Nuctech is owned by Tsinghua Tongfang Co., a state-owned software company which itself is owned by Tsinghua Holdings, a subsidiary of Tsinghua

¹ <http://www.nuctech.com/en/SitePages/SeNormalPage.aspx?nk=ABOUT&k=ACABGD>

² <https://www.chinaeducenter.com/en/cedu/ceduproject211.php>

³ <http://www.nuctech.com/en/SitePages/SeNormalPage.aspx?nk=ABOUT&k=DGEAGA>

⁴ <https://www.streetinsider.com/Press+Releases/Tsinghua+University+and+Nuctech+Co-constructed+Chinese+National+Engineering+Laboratory+for+Dangerous+Articles+and+Explosives+Detection+Technologies/13744785.html>

University, and the China National Nuclear Corporation, a state-owned entity whose President and Vice President are directly appointed by the Premier of the PRC.⁵

In addition, many private and state-owned companies in China include “party committees”, which are formed by senior CCP members and given broad authority as part of executive teams and/or boards of directors.⁶ Nuctech, as an important exporter of Chinese technology to foreign countries, would most assuredly include one of these committees within its leadership structure.

All of these connections provide a startlingly open avenue for the PRC to exert control over Nuctech. These connections are too integrated and deeply woven into Nuctech’s operations to ignore the possible security concerns.

The Power and Control of China

These relationships to the Chinese government would not themselves raise concerns if not for China’s current information security policies and their history of espionage with foreign technology companies.

Under the Cybersecurity Law of the People’s Republic of China enacted by the Standing Committee of the National People’s Congress of China on November 7, 2016, China requires network operators within China to store select data and submit said information to Chinese authorities, should the data be requested.⁷ Online services such as Skype and WhatsApp have since either been restrained from further expansion in China or banned entirely for refusing to cooperate with this law. The law has raised concerns among western social activists and companies either operating or seeking to operate within China. Nuctech, as a Chinese company with close ties to the Chinese government, could be required to store and provide data to the Chinese government upon request; there would be no way to object to data being passed through Nuctech machines outside of China.

China also has a history of hacking and foreign espionage. In 2016, Su Bin – a Chinese national – pleaded guilty to participating in a years-long conspiracy to hack networks of major U.S. defense contractors to steal sensitive military data.⁸ China has been implicated in an alleged hack of the UK defense firm BAE Systems that began in 2014, attempting to infiltrate supply chains and steal sensitive data.⁹ China has also been implicated in the

⁵ https://en.wikipedia.org/wiki/China_National_Nuclear_Corporation

⁶ <https://thediomat.com/2019/12/politics-in-the-boardroom-the-role-of-chinese-communist-party-committees/>

⁷ <https://thediomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>

⁸ <https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive>

⁹ <https://www.bbc.com/news/technology-39478975>

2004 attack on the former Canadian technology firm Nortel that ended up pushing Nortel into bankruptcy in 2009.¹⁰

China has shown its willingness to perform foreign espionage and large-scale hacking operations in an effort to compromise foreign networks and pilfer sensitive data. It is probable that, should the PRC see value in obtaining sensitive data using Nuctech systems deployed abroad, they will not hesitate to do so.

A History of Unethical Business Practices

Nuctech itself has a history of questionable business practices in foreign nations that call into question its integrity.

In 2009, Nuctech was implicated in a bribing and corruption scandal in Namibia. A report of large money transfers was reported to Namibia's Anti-Corruption Commission; 9M€ was transferred to a Namibian firm called Teko Trading. This was believed to be a bribe to allow Nuctech to secure a contract worth 39M€ with the Namibian government.¹¹¹² Meanwhile, Chinese censors removed all mention of the scandal within China, allegedly in an effort to protect former Nuctech chair Hu Haifeng.¹³

In 2009, a London-based x-ray scanning firm, Smiths Detection, accused Nuctech of dumping (selling products at prices significantly below market value) into the EU market in an effort to gain greater market share using their advantageous ties to the Chinese government and their ability to sell far below EU market value. Their complaint, submitted to the European Trade Commission, prompted the commission to impose a 36.6% provisional duty on large-scale cargo-scanning equipment from China in December of that year.¹⁴ The British firm called into question the security of using Nuctech scanning machines across the EU and the unfair connections Nuctech has with the Chinese government, allowing them to vastly undercut competition with little risk to themselves.

Nuctech was also involved in a corruption and honeypot scandal in Taiwan. In 2016, Sun Yi-Ming, the former head of the Aviation Police Bureau's aviation security section in Taiwan, was found guilty of corruption and sentenced to over 17 years in prison. He was convicted of receiving kickbacks and engaging in illicit activities relating to a \$70M contract to acquire x-ray scanners from Nuctech. Nuctech itself is said to have sent a female sales manager to execute a honeypot trap on Sun Yi-Ming and obtain information about the project. Sun Yi-Ming was also found to have aided Nuctech in creating a sham presented to Taiwanese regulators by having Nuctech machines reassembled in Japan.

¹⁰ <https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel/>

¹¹ <https://www.dw.com/en/chinese-firm-embroiled-in-namibian-corruption-scandal/a-5213591>

¹² <https://www.nytimes.com/2009/07/22/world/africa/22namibia.html>

¹³ <https://www.csmonitor.com/World/Asia-Pacific/2009/0803/p06s01-woap.html>

¹⁴ <https://www.nytimes.com/2010/04/28/business/global/28iht-trade.html?auth=login-google>

During the investigation, Nuctech machines were suspected to contain embedded software for sending data and images to China. Airport security in Taiwan took to calling the four already installed Nuctech scanners “blind x-ray scanners” due to their frequent breakdowns and poor detection performance.¹⁵

This history of disreputable business dealings calls into question Nuctech’s ethics along with its business ventures. Any deals made with Nuctech must consider this history and the fact that Nuctech has not, as of yet, shown a willingness to commit to more fair and ethical business practices.

Poor Quality Manufacturing and System Functionality

Nuctech machines are alleged to be of poor quality and sub-par performance. As previously mentioned, Taiwanese airport officials have referred to Nuctech scanners as “blind x-ray scanners” precisely because of their frequent breakdowns and inability to detect certain items.¹⁶ Because of this and other evidence gathered by the U.S. Government, the U.S. Department of Homeland Security does not allow any goods scanned by Nuctech x-ray systems to be transported on flights to the United States.

The government of Lithuania, in January of this year, set to block Nuctech from installing scanners in their country. A parliamentary appointed committee concluded that Nuctech’s baggage and cargo scanning equipment did not meet national security standards in Lithuania, and blocked the signing of a contract with Nuctech to install scanners in three (3) of the country’s international airports.¹⁷

In addition, in a rule implemented December 18, 2020, the U.S. governments’ Bureau of Industry and Security added Nuctech to its Entity List, a supplement to the Export Administration Regulations meant to identify entities “...for which there is reasonable cause to believe based on specific and articulable facts, that the entities have been involved, or pose a significant risk of becoming involved in activities contrary to the national security and foreign policy interests of the United States.” The report, released on December 22 by the End User Review Committee, found that “...Nuctech’s lower performing equipment impair U.S. efforts to counter illicit trafficking in nuclear and other radioactive materials. Lower performing equipment means less stringent cargo screening, raising the risk of proliferation.”¹⁸

¹⁵ <http://www.taipeitimes.com/News/taiwan/archives/2020/02/28/2003731760>

¹⁶ 15, ibid

¹⁷ <https://illinoisnewstoday.com/lithuania-set-to-block-chinese-airport-scanner-company-nuctech-wgn-radio-720/46436/>

¹⁸ <http://www.govinfo.gov/content/pkg/FR-2020-12-22/pdf/2020-28031.pdf>

Nuctech's lowered standards and sub-par equipment call into question the effectiveness of a scanning system including or based on Nuctech hardware. Any inclusion of Nuctech systems can be a critical security risk and a potential vector of vulnerability.

U.S. Government Concerns Regarding China and Nuctech

The U.S. government has made clear the security concerns it has with Chinese technology firms and Nuctech specifically, and has made efforts to press other nations to deny these Chinese companies access to foreign contracts.

American agencies have led a campaign, headed by the National Security Council (NSC), to uproot Nuctech from its placements throughout Europe. Nuctech has become a fixture across Europe, utilized in many ports, airports, and border crossings. The NSC argues that Nuctech security is unreliable, and cites concerns over Nuctech's connections in China, and the security risk that poses to foreign nations. As previously stated in this brief, we believe those concerns are warranted and reasonable.¹⁹

In more broad terms, the FBI, in a March 2020 statement before the Senate Judiciary Committee Subcommittee on Crime and Terrorism, outlined the cyber-threats originating from China. The FBI states, "While several nation-states pose a cyber threat to U.S. interests, no other country presents a broader and more comprehensive threat to our ideas, innovation, and economic security than the People's Republic of China (PRC) under the leadership of the Chinese Communist Party (CCP)." The FBI cites the 2017 Chinese hack of Equifax, executed by four Chinese cyber-actors who allegedly acted as agents of the PRC People's Liberation Army. The statement also mentions the threat of Chinese companies, China's 2017 cyber-security law, and the risk of foreign data collection.²⁰

The U.S. Government has clearly stated its concerns regarding China's technology firms, and the very integrated role of the Chinese government in these companies. Any ongoing FBI investigations are not yet known, but it is likely that the FBI and other U.S. federal agencies have more evidence that may be a cause for concern regarding Nuctech and Chinese technology as a whole.

Protecting National Security

International security experts and the media have expressed increasing concern over the Chinese security threat to the Western world. Heightened awareness of questionable operations by Chinese-owned security agency, Nuctech, have caused global security officials to publicly express apprehension over the use of backdoor technology to pass on sensitive data – manifests, security images, personal information and more – to the Chinese government. Nuctech, with close ties to both the Chinese government and

¹⁹ <https://www.wsj.com/articles/u-s-presses-europe-to-uproot-chinese-security-screening-company-11593349201>

²⁰ <https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing>



military, has practiced unfair business strategies, bribery, sharing sensitive data, and widespread corruption. Now countries around the world are following the U.S. decision to blacklist Nuctech, protecting sensitive data information and further harnessing national security.

Astrophysics Company Overview

Astrophysics has led the global security industry in research and development, creating integrated solutions and customized products that advance the critical security missions of our customers and partners. For nearly two decades, American x-ray manufacturer Astrophysics Inc. has built a respected reputation for ethical business practices and protecting sensitive customer data. Known for quality and innovative technology, Astrophysics develops world-class x-ray scanners, and has deployed over 30,000 x-ray systems at critical infrastructure sites, airports, and ports and border crossings in over 150 countries worldwide.



HQ
+1.909.598.5488

EMEA
+961.9.832.500/1/2

ASIA
+63.2.812.0033

INDIA
+91.11.41709990

www.astrophysicsinc.com