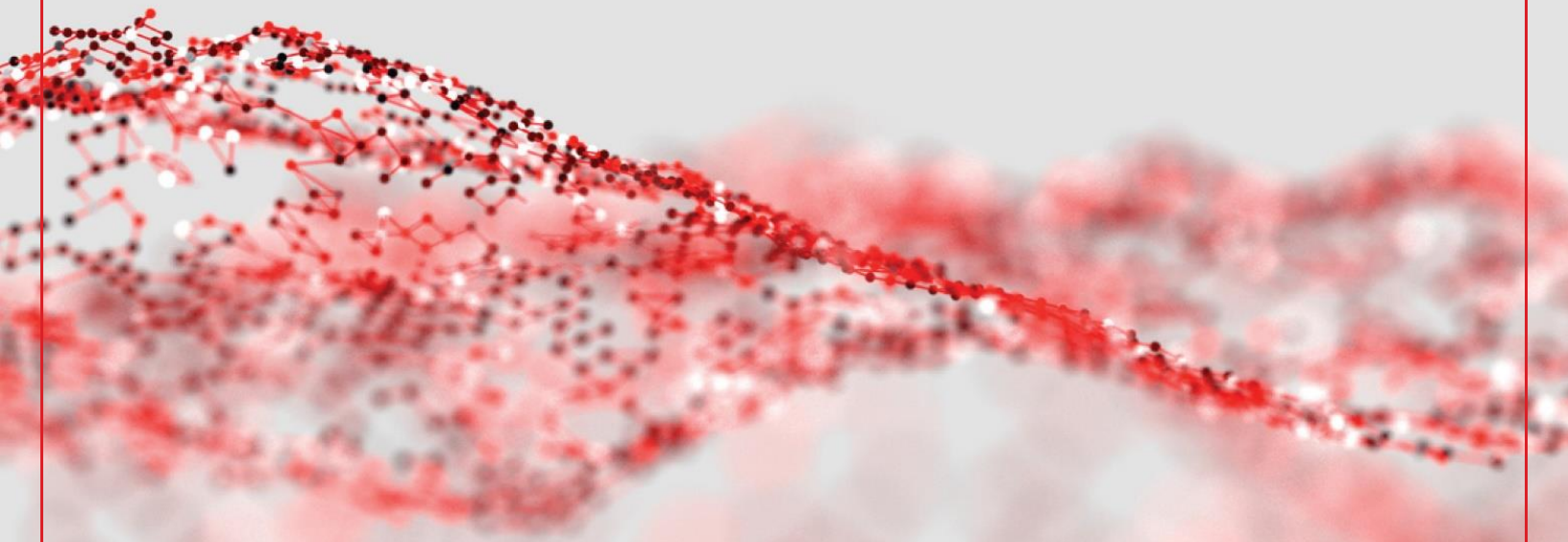
# CFIUS' Growing Power to Protect American Security from China Tech Threats:

## Examining TikTok and Lenovo

June 26, 2020



China TECH THREAT

PARLIAMENTARY INTELLIGENCE-SECURITY FORUM

# CFIUS' Growing Power to Protect American Security from China Tech Threats:
## Examining TikTok and Lenovo

## TABLE OF CONTENTS



## CO-AUTHORS


**Dr. Roslyn Layton, PhD**
**Co-Founder, China Tech Threat**
*A Visiting Researcher at Aalborg University Center for Communication, Media, and Information Technologies and a Vice President at Strand Consult, both in Denmark. She is a Visiting Scholar at the American Enterprise Institute in Washington, and served on the President Elect Transition Team for the Federal Communications Commission (FCC). In the popular press, she has been published in The Wall Street Journal, US News & World Report, and Forbes, among others. Dr. Layton has a Ph.D. in business economics from Aalborg University, an M.B.A. from the Rotterdam School of Management (Netherlands), and a B.A. in international service from American University.*

**Robert Pittenger**
**Former Chairman, Congressional Taskforce on Terrorism and Unconventional Warfare**
*From 2013-2018, Congressman Pittenger represented the Charlotte, NC area with a focus on national security, foreign investment reform, tax reform, and religious freedom. At the time, he served as Chairman of the Congressional Task Force on Terrorism and Unconventional Warfare, and as Vice Chairman of the House Financial Services Subcommittee on Terrorism and Illicit Finance. Congressman Pittenger was a lead author of the 2018 Foreign Investment Risk Review Modernization Act (FIRRMA), which reformed the Committee on Foreign Investment in the United States (CFIUS) to crack down on malicious foreign investment targeting national security technology. Today he is Chairman of the Parliamentary Intelligence-Security Forum, which has brought together over 1500 Members of Parliament and other leaders from 106 countries in Europe, Africa, Asia, and South America to discuss counter-terror finance, cyber security, data sharing, cryptocurrencies, and predatory foreign investment.*

## EXECUTIVE SUMMARY:

Beginning in 2017, the executive branch agency CFIUS (Committee on Foreign Investment in the United States) has stepped up in an unprecedented way to protect American security from investors owned or affiliated with the Chinese government. First, in response to a tripling of investment from China, CFIUS has become more rigorous in the number of investigations it undertakes and the number of transactions withdrawn. Second, in 2018, Congress significantly expanded CFIUS' resources and scope to empower the agency to safeguard Americans' personal information and the nation's technological and industrial advantages.

Consequently, purchases of strategic American businesses by Chinese interests have been blocked, notably Alibaba's Ant Financial purchase of MoneyGram – an opposition led by Rep. Pittenger; or divested from their Chinese owners, including US companies PatientsLikeMe, Grindr, and StayNTouch. In his Congressional career, Rep. Pittenger also led efforts to end the use of Lenovo products by the US Air Force and the blockage of the Chinese purchase of the Chicago Stock Exchange.

This paper explores two key recent transactions: the on-going review of ByteDance's purchase of TikTok, and CFIUS' approval of Lenovo's acquisition of strategic IBM and Motorola assets, despite vehement opposition from Congress and defense and intelligence agencies. The Lenovo acquisitions catalyzed bi-partisan reform of CFIUS with the *Foreign Investment Risk Review Modernization Act* of 2018 (*FIRRMA*). Under the new cybersecurity and personal information factors CFIUS must consider today, the Lenovo acquisitions of the past would probably not have been approved.


## OVERVIEW: CFIUS' JOB IS TO PROTECT AGAINST THE LOSS OF ADVANTAGE IN STRATEGIC TECHNOLOGICAL ASSETS

In 2015 the Chinese government announced its "Made In China 2025" initiative, a plan for China to conquer the US as the world's technological leader and to dominate the core technologies of the future. This is underpinned by China's larger "techno-nationalist" strategy of projecting global power through its corporate tech champions and accumulating hard currency through the sale of consumer goods and electronics to support its military projects around the globe and in space.

China Tech Threat
Roslyn Layton – roslyn@chinatechthreat.com

Parliamentary Security-Intelligence Forum
Robert Pittenger – Alex@pi-sf.com

The technology that China can't develop itself, it will acquire—with a preference for leading brands. The technology China can't acquire, it will steal. China's documented strategy of "unrestricted warfare" includes significant information operations toward the US: the theft and hacking of intellectual property; surveillance and espionage of sensitive and strategic information activities; the collection and processing Americans' personal information; and the set of illegal practices like forced technology transfers, predatory pricing, strong-arm sales tactics, bribery, fraud, and corruption.

One element of China's plan is to purchase tech assets from U.S. businesses, some of which may be crucial for US national security. Until recently, the Committee on Foreign Investment in the United States (CFIUS), a body comprised of nine cabinet-level Executive Branch agencies and offices charged with reviewing the national security aspects of foreign direct investment, lacked sufficient resources and jurisdiction to do its job. Now with information privacy and security standards clarified, review process improved, and budget increased, CFIUS has stepped up to defend Americans in the face of foreign actors which could use their data for subversion, exploitation, extortion, espionage, and other crimes.

## CFIUS' SCOPE AND PROCESS

The scope of CFIUS is appropriately limited to its narrow jurisdiction of "covered transactions," specifically mergers, acquisitions, joint ventures, leases, and other investments where foreign persons/entities contemplate buying or making an investment and could result in foreign control of a US business and credible evidence to suggest that the entity could take an action to threaten or impair national security. CFIUS can block, modify, and unwind transactions, and advise the President on national security matters. Notifying CFIUS of a pending investment is voluntary but failing to do so entails a risk that CFIUS will undertake an investigation after a transaction is complete.

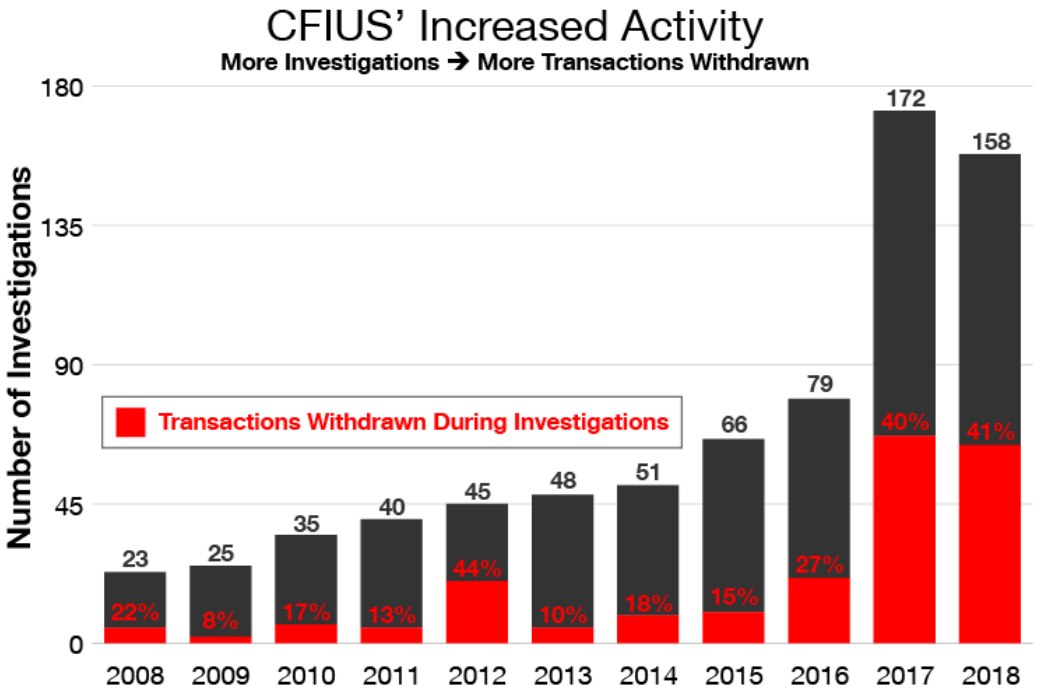
The baseline for CFIUS reviews includes the following parameters: (1) whether the US business has a national security responsibility or has performed classified contracts in the past, (2) whether the US business has critical technologies/products (commodities, software, or technology controlled under US export control laws); (3) whether the transaction would result in foreign control, physical or virtual, of critical infrastructure, and (4) whether the US business has locations near sensitive government facilities.

## INCREASED CFIUS SCRUTINY, BEGINNING IN 2017

Recent CFIUS reports to Congress highlight the Committee's dramatically increased activity beginning in 2017 and continuing in 2018, the last year for which public information is available. For starters, the number of investigations more than doubled from 79 in 2016 to 172 in 2017 and remained higher, with 159 in 2018. During the same period, withdrawal notices tripled from 21 to 67 and then stayed at a higher level of 64. By expansion, there were only 76 such withdrawal notices *combined* in the 7 prior years (2010-2016), roughly the same number of withdrawal notices in each of the past two years.

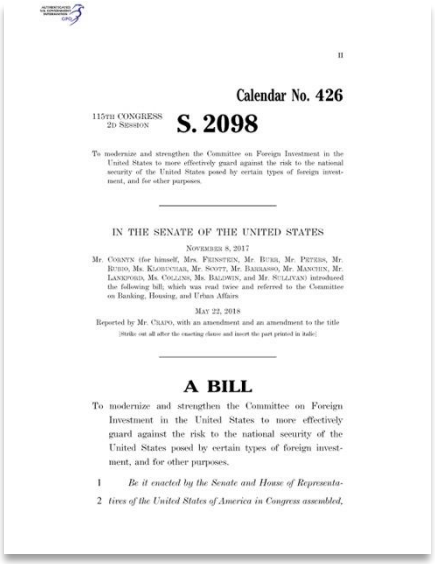
It is important to study the number of withdrawn transactions because this is an indicator that CFIUS is effectively stopping deals that threaten US security. After all, the main reasons parties would withdraw (besides a change in commercial motivation) are because of unresolved national security concerns, or the parties do not want to abide by CFIUS's proposed mitigation, or a decision by CFIUS to refer the matter to the President – which would likely result in rejection. (Note: parties may withdraw to provide additional time to resolve concerns and reapply.)

Finally, as a specific indicator of CFIUS' capacity to stop deals that are harmful to national security, the agency began reporting the number of transactions abandoned because of national security concerns in 2015. While there were only 3 cases in 2015 and another 3 the following year, in 2017 the number jumped to 24 – an 8-fold increase – and remained at 18 in 2018. Evidently, CFIUS is increasingly thwarting the foreign purchase of strategic companies important to America's national security.




The Bureau of Economic Analysis reports that more than two-thirds of the total foreign investment in the US comes from European investors; perhaps less than 5 percent of foreign investment comes from investors from adversarial states. As such, the purview of CFIUS is necessarily and appropriately limited. Most investments reviewed by CFIUS are approved with some mitigation. However, with credible evidence of threat, investments can be blocked and divested. While CFIUS may have blocked deals in the past in which the Chinese government was an investor in a strategic business, it has also approved many such deals. For this and related reasons, there was a policy concern that CFIUS was a "black box" and its review criteria and process were opaque and subjective. FIRRMA instituted reforms to improve the process and transparency of CFIUS and to increase its budget for more people and resources to conduct reviews. CFIUS must also review transactions against a set of factors that weigh cybersecurity and information privacy.

## FIRMMA EXPANDED CFIUS IN 2018



II

Calendar No. 426

115TH CONGRESS
2D SESSION

**S. 2098**

To modernize and strengthen the Committee on Foreign Investment in the United States to more effectively guard against the risk to the national security of the United States posed by certain types of foreign investment, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 8, 2017

Mr. CORNYN (for himself, Mrs. FEINSTEIN, Mr. RUBIO, Mr. PETERS, Mr. RUBIO, Ms. KLOBUCHAR, Mr. SCOTT, Mr. BARRASSO, Mr. MANCHIN, Mr. LANKFORD, Ms. COLLINS, Ms. BALDWIN, and Mr. SULLIVAN) introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

MAY 22, 2018

Reported by Mr. CRAPO, with an amendment and an amendment to the title

[Strike out all after the enacting clause and insert the part printed in italic]

**A BILL**

To modernize and strengthen the Committee on Foreign Investment in the United States to more effectively guard against the risk to the national security of the United States posed by certain types of foreign investment, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

Led by former Representative Robert Pittenger (NC) and current Senator John Cornyn (TX), Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018 with broad bipartisan support. While FIRRMA recognized the benefits of foreign investment to the US economy and the fact that the top seven investor states are long-standing US allies, a distinct set of foreign investments pose increased risk to the national security. The bill thus amended earlier legislation to increase CFIUS' authority to review national security implications of foreign investment. In recent years, China's increased techno-military fusion and investment in strategic businesses in the US, has triggered CFIUS scrutiny.

FIRRMA made important changes to improve the effectiveness of CFIUS. These include a budget[1] of $20 million and expanded staff. Cooperating agencies have also increased their budgets and staff to coordinate with CFIUS, notably the Department of Justice (DOJ) through its China Initiative[2] focusing on identifying and prosecuting economic espionage, trade secret theft, hacking and other economic crimes. After some years of relative disinterest in China's economic crimes against the US, DOJ has brought some 50 cases in the last two years alone.

FIRRMA centralizes CFIUS operations in the Treasury Department, creating two new Senate-appointed positions in the department responsible for overseeing CFIUS operations. FIRRMA also requires CFIUS to have dedicated staff, including an Assistant Secretary or equivalent position. Importantly, CFIUS' scope is expanded to noncontrolling investments in critical technology, critical infrastructure, and collecting personal data, among other indicators.

FIRRMA also added critical factors which CFIUS must consider in conducting reviews including

- whether the transaction is likely to reduce the technological and industrial advantage of the United States relative to adversaries
- whether the transaction is likely to contribute to the loss of or other adverse effects on critical technologies which provide the US a strategic national security advantage
- degree to which the transaction will increase the cost of the US government to acquire or maintain equipment and systems for defense, intelligence, or other national security functions
- the extent to which the covered transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security;
- whether the covered transaction is likely to have the effect of creating any new cybersecurity vulnerabilities in the United States or exacerbating existing cybersecurity vulnerabilities;

[1] Treasury, U. O. (2020). Committee on Foreign Investment in the United States. Retrieved 2020, from https://home.treasury.gov/system/files/266/10.-CFIUS-FY-2021-BIB.pdf

[2] International Studies, C. A. (2020, February 6). CHINA INITIATIVE CONFERENCE. Retrieved 2020, from https://www.justice.gov/opa/gallery/china-initiative-conference?_sm_au_=iVV56DJnJRWnrDv001TfKK3Qv3fc4

- whether the covered transaction is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States, including such activities designed to affect the outcome of any election for Federal office;
- whether the covered transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology that a United States business that is a party to the transaction possesses.

In January 2020, CFIUS issued rules to clarify FIRMMA implementation in two ways. First, CFIUS expanded jurisdiction over non-controlling interests by foreign governments in strategically important U.S. businesses in critical technology, key infrastructure or sensitive personal data. Second, CFIUS specified real estate transaction rules by a foreign person near specific airports, maritime ports, and military installations.[3] Pivotal in this implementation of FIRMMA were Richard Ashooh, Assistant Secretary of Commerce-Bureau of Industry and Security, and Thomas Feddo, Assistant Secretary of the Treasury for Investment Security.

## CFIUS' TRAIL OF RECENT BLOCKED TRANSACTIONS

CFIUS review is hardly confined to investments originating in China. Countries which are key allies and investors in the US are also subject to review, including Japan, Canada, France, and some 50 others. Over the years, both Democrat and Republican administrations have blocked Chinese investment, frequently but not always in because of the presence of a Chinese government-owned investor.

For example, in 1990 the sale of Seattle-based Mamco to a the state-owned China National Aero-Technology Import & Export Corp. (CATIC) was voided because President Bush believed the Chinese government was "trying to get military secrets[4]." In 2005, Congress blocked a Chinese state owned energy company from buying Unocal. CFIUS has scuttled Huawei's investments in the US with Bain Capital LLC in 2008 and with 3Com and 3Leaf Systems in 2011.

In 2016, President Obama acting on CFIUS's recommendation, blocked acquisition of Aixtron Semiconductor by a German company which itself was to be acquired by a Chinese government-owned investment fund.

In any case, CFIUS review has not slowed Chinese investment. Indeed, investment from China in the US tripled to $40 billion from 2015 to 2016 and remained at that level for 2017 and 2018. It is logical that CFIUS would increase oversight of Chinese investment following increased investment. Moreover,

---

[3] Treasury, U. O. (2020). Committee on Foreign Investment in the United Staes. Retrieved 2020, from https://home.treasury.gov/system/files/266/10.-CFIUS-FY-2021-BIB.pdf

[4] Auerbach, S. (1990, February 3). President Tells China to Sell Seattle Firm. Retrieved 2020, from https://www.washingtonpost.com/archive/politics/1990/02/03/president-tells-china-to-sell-seattle-firm/4e2521e2-3ba1-4d9b-a864-ec512a607a28/

China's aggressive overtures to the US and its increasing militarization against US interests also justify the increase in CFIUS activity.

The ascent of General Secretary Xi Jingping is marked with China's increases in authoritarianism and censorship; repression in Hong Kong, Taiwan and Tibet; and belligerence in the South China Sea, a key trade route. The country also adopted sweeping new laws asserting China's sovereignty and authority over cyberspace and the data of Chinese information technology (IT) companies. As such, it is necessary that CFIUS has increased its scrutiny of acquisitions in the IT domain and to stop transactions which threaten Americans' privacy and security.

In 2018 CFIUS blocked the purchase of MoneyGram by the Alibaba's Ant Financial because of concern that Americans' financial information could be exposed to the Chinese government. American law has strong, historical protections for sensitive and personal information such as health, genetics, gender, and sexual orientation, and in 2019 CFIUS forced the divestiture of two tech acquisitions by Chinese interests which it determined put Americans' personal information at risk for exploitation.

This included PatientsLikeMe, a patient-network and research platform in which people with similar diseases connect online, and the gay dating app Grindr which collected geolocation and HIV status. In 2020, presumably based on concerned of personal data of hotel guests, President Trump himself ordered that Beijing Shiji Information Technology Co., Ltd. divest its interest in StayNTouch, Inc. a U.S. company providing mobile technology and property-management systems for hotels.

Indeed, using FIRRMA's stricter standards for privacy and security, earlier approved deals which involved Chinese government investment would likely not be approved today, such as the multibillion-dollar acquisition of IBM's laptop and server division by Lenovo, which the United States China Commission (USCC) considers one of China's national tech champions on the order of Huawei.

## CASE STUDY #1:

### CFIUS' New Strength: Putting the Brakes on Beijing's Control of TikTok

In October 2019, Florida Senator Marco Rubio requested[5] CFIUS to investigate TikTok, the short-video app acquired by the Chinese backed ByteDance. Soon thereafter senators Chuck Schumer (D-New York) and Tom Cotton (R-Arkansas) wrote[6] to the US Director of National Intelligence about the company. The following month CFIUS opened[7] an investigation.

In addition to chilling reports of the Chinese government censoring TikTok videos which had discussions of human rights protests in Tiananmen Square, Tibet, Hong Kong, and Taiwan, the app collects extensive personal and sensitive information such as user location, name, age, and IP address. Earlier in 2019, the Federal Trade Commission issued[8] a $5.7 million fine to TikTok's illegal collection of information from children, the largest settlement to date of the Children's Online Privacy Protection Act. Given the sensitive nature of geolocation for military personnel, the Department of Defense banned[9] the use of TikTok by the military, and Missouri Senator Josh Hawley proposed[10] legislation to ban its use by federal employees.

TikTok has repeatedly denied that the Chinese government exercises control over the firm, but a series of interviews with former employees suggests otherwise.[11] Plus documents leaked[12] to the press describe how content is routinely censored based upon political subject and any reference to China's General Secretary Xi Jingping.

The existence of the Chinese government's database of Americans' personal information has been known and described for years.[13] US authorities have verified that hacks of Office of Personnel Management (OPM), Anthem health insurance, and Marriott were carried out by the Chinese government, notably the cyber arm of the People's Liberation Army.

The 2014 hack of OPM, the human resources office of the federal government, exposed more than 20 million records of current and former federal employees, including the identity of 3 million workers with security clearances and those which US employees met with Chinese officials. In additional to gaining more information about the US, China's goal is to screen the data to recruit potential spies for the Chinese

---

[5] Marco Rubio, O. S. (2019, October 9). Rubio Requests CFIUS Review of TikTok After Reports of Chinese Censorship. Retrieved 2020

[6] Tom Cotton, O. S. (2019, October 24). Cotton, Schumer Request Assessment Of National Security Risks Posed By China-Owned Video-Sharing Platform, TikTok, A Potential Counterintelligence Threat With Over 110 Million Downloads In U.S., Alone.

[7] Alper, A., Roumeliotis, G., Wang, E., & Yang, Y. (2019, November 1). Exclusive: U.S. opens national security investigation into TikTok - sources. Retrieved 2020

[8] Commission, F. T. (2019, February 27). Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law. Retrieved 2020

[9] Vigdor, N. (2020, June 4). U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning. Retrieved 2020

[10] Josh Hawley, O. S. (2020, March 4). TikTok, National Security Threats the Focus of Hawley's 'Dangerous Partners: Big Tech and Beijing' Hearing. Retrieved 2020

[11] Hartwell, D. (2015, November 6) Inside TikTok**:** A culture clash where U.S. views about censorship often were overridden by the Chinese. *The Washington Post.*

[12] Hern, A. (2019, September 25). Revealed: How TikTok censors videos that do not please Beijing. *The Guardian.*

[13] Nakashima, E. (2015, June 6) With a series of major hacks, China builds a database on Americans. *The Washington Post.*

government and to gather information which can be used for social engineering, a form of deception and manipulation of individuals who offer access to valuable information and assets.

One notable social engineering exploit was perpetrated on Boeing employees to infiltrate the companies secure systems and acquire the Department of Defense's secret plans for fighter jets. The hack of Marriott, one of the most frequented hotels by US government and military employees, was also significant because it exposed 500 million records.

In May 2020, *Reuters* reported[14] that TikTok is moving operations out of China to the US. Key management in Beijing have left the firm, and it appears that they are not transferring to the US to run the company. It is not clear whether the move is the direct result of a CFIUS requirement or whether it is a proactive effort to demonstrate that TikTok is not controlled by the Chinese government. While the move itself is symbolic, it does not mitigate the cybersecurity and privacy risks.

It does not matter where the data is processed or stored. As long as TikTok is a Chinese-owned company, it can be compelled by the Chinese government to collect, process, store, or transfer data to the Chinese government. This is a common feature of any Chinese IT company working in the US. Emmanuel Pernot-Leplay, PhD in comparative

**Timeline of Key TikTok Events**

| | |
|---|---|
| May 2017 | TikTok launched for the first time in the global market; app targets Western markets instead of Chinese mainland. |
| November 2017 | TikTok parent company ByteDance acquires Musical.ly in the US for $1billion; acquires Musical.ly's 100 million users in the acquisition. ByteDance fails to inform CFIUS of transaction. |
| September 2019 | TikTok becomes the #1 free non-gaming app in the United States. |
| October 2019 | U.S. Senate Minority Leader Chuck Schumer and Senator Tom Cotton ask intelligence officials to investigate whether TikTok poses a national security risk. |
| November 2019 | CFIUS open probe of TikTok over ByteDance acquisition stating national security and data privacy concerns as reasons for inquiry. |
| December 2019 | Defense Department Cyber Awareness Memo identifies TikTok as "having potential security risks associated with use;" DOD and US Armed Forces ban use of app in weeks after. |
| May 2020 | Multiple Congressional bills introduced to ban Federal employees' use of TikTok, citing concerns about sensitive and personal data. |

[14] Yang, Yingzhi, et al. (28, May 2020). "Exclusive: TikTok Owner ByteDance Moves to Shift Power out of China - Sources." *Reuters*

data protection law[15] from Shanghai Jiao Tong University put its best: "Governments worry less about what Chinese law says than what China's government can actually do." For that reason, NATO, the US military, and the US federal government restrict their use of IT products and services from Chinese state-owned and affiliated entities.

## CASE STUDY #2:

### The One That Got Away: CFIUS Today Would Likely Have Stopped Lenovo's IBM Purchases

Over the years, CFIUS decisions have been harshly critiqued, notably for approving mergers against the vehement opposition of Congress, the Department of Defense, the Department of Homeland Security, and other national security actors. This has led some observers to critique the process and criteria of CFIUS review, itself an important driver of the major CFIUS reform adopted in 2018.

> "IBM has systematically transferred high-end computing technology to China. By 2016, according to a working group of experts from the National Security Agency and Energy Department, China had "attained a near-peer status with the U.S." in high-performance computing. Without a doubt, IBM's technology transfers have contributed to China's enhanced high-performance computing capabilities."
>
> - Robert Pittenger, 3/14/18
> *Wall Street Journal*

Some of the most contested CFIUS reviews involve the Chinese government owned Lenovo, which succeeded to purchase multiple US assets and transform itself into the world's leading maker or laptops and a global leader in servers and smartphones. Lenovo and its US partners IBM, Google, and Motorola purposely billed the assets as "low-end commodities" to downplay, if not dismiss, national security concerns and to effect quick CFIUS approval without involving Congress or the President. This also fit the prevailing business elite ethos that the US should outsource manufacturing because it is inherently "low value." This view is being revisited particularly as the US faced major shortages of critical goods during the COVID-19 pandemic. Moreover, supply chain security garners increasing importance for information technology goods and services.

A management research inquiry to the earlier acquisitions might show that while IBM, Motorola, and Google had little use for the set of strategic assets, other firms in the US and allied countries could have made use of them—had they the chance to bid. Indeed, other CFIUS reviews have required such mitigation, in which the US firm finds a buyer which does not pose a privacy or security threat.

In *The Lenovo affair: the growth of China's computer giant and its takeover of IBM-PC* by leading Chinese business journalist Ling Zhijun describes what the Lenovo acquisition of IBM meant from the Chinese perspective. "To China, this acquisition was not only unprecedented in Chinese history, it was a portent of China's gaining superiority in a fierce competition." The acquisition transformed Lenovo into the "IBM of China." Despite its 55 percent Chinese government ownership in 2005 (now reduced to 29 percent), Lenovo has made 4 strategic technological acquisitions in the US, all passing CFIUS review. During this period Canada rebuffed Lenovo's attempt to acquire Blackberry.

---

[15] Leplay, Emmanuel Pernot. (9, March 2020). "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?" Penn State Journal of Law & International Affairs, vol. 8, no. 1.

When Lenovo and IBM appeared before CFIUS in 2014 with the deal to acquire IBM's x86 server business for $2.3 billion, they had a decade of practice with the CFIUS process and Washington's most skilled lawyers and lobbyists to argue their case. This was important to find a way to consummate a deal despite IBM's servers being deployed in sensitive US military and weapons installations like the Aegis Combat System, the integrated naval weapons system produced by Lockheed Martin which uses powerful computer and radar technology to track and guide weapons to destroy enemy targets.[16]

The US Navy noted the increased security risk of the Lenovo deal and its need to shed the IBM x86 BladeCenter server because of the Navy's ballistic, anti-air warfare, missile defense capability, and guided missile cruiser and destroyer fleets.[17] Aegis is deployed by navies in Japan, Spain, Norway, South Korea, Australia, and in NATO's missile defense. The IBM server is also a part of Raytheon's GPS Next-Generation Operational Control System, known as GPS OCX, Global Positioning System (GPS).[18]

As part of the mitigation, IBM agreed to provide maintenance for the military servers for 5 years until they would be turned over to Lenovo, upgraded or removed. The acquisition was approved, though the cost to rip and replace GPS servers was not borne by Lenovo, IBM, or Raytheon.

Taxpayers are still on the hook today, with the latest cost being $378 million to rip and replace the Air Force/Space Force servers which otherwise would be under the potential purview of the Chinese governments.[19] Separately, IBM x86 servers were also part of major international internet hubs and backbones run by US firms, but were not required to be removed or mitigated as part of the acquisition.

## FIRRMA FACTORS APPLIED TO LENOVO

FIRRMA mandated that CFIUS must include a set of factors related to personal data and cybersecurity in its review. These factors have special implications for acquisitions related to information technology as noted in the following table. Given the increased important of these factors, it is likely that the Lenovo acquisitions would not have been approved if they were held to the new standards. Instead of selling to Lenovo, IBM could have sold its laptop and server divisions to one of many companies based in the US or allied countries.

| FIRRMA Requirements for CFIUS Review | Lenovo acquisitions of IBM ThinkPad laptop 2004 and IBM x86 servers 2014 |
|---|---|
| Whether the transaction is likely to reduce the technological and industrial advantage of the United States relative to adversaries | Today Lenovo is the world leader in laptop manufacturing and sales with 25%[20] of world's market share, supplanting IBM |
| Whether the transaction is likely to contribute to the loss of or other adverse effects on critical technologies which provide the US a strategic national security advantage | Before the internet and the explosion of data collection, laptops and servers may have been considered lesser security risks. Today, however, these devices store massive amounts |

[16] Martin, L. (n.d.). Aegis: The Shield of the Fleet.

[17] Eckstein, M. (2015, May 5). Navy Needs New Servers for Aegis Cruisers and Destroyers After Chinese Purchase of IBM Line. Retrieved 2020

[18] "GPS Next-Generation Operational Control System." *Raytheon Intelligence and Space*

[19] (2020 March 27) "Raytheon Gets OK, $378 million to Replace Risky OCX Hardware" *Breaking Defense*

[20] Hanson, Matt. "Lenovo Maintains Lead in PC Market Share, but Apple Is Catching Up." Tech Radar, 12 July 2019

| FIRRMA Requirements for CFIUS Review | Lenovo acquisitions of IBM ThinkPad laptop 2004 and IBM x86 servers 2014 |
|---|---|
| | of sensitive data, particularly in decrypted form. Moreover, these devices conduct cloud services linking multiple databases with massive amounts of sensitive and personal information at risk |
| Degree to which the transaction will increase the cost of the US government to acquire or maintain equipment and systems for defense, intelligence, or other national security functions | US government and taxpayers suffered increased cost from ripping and replacing the equipment, an undisclosed amount for Aegis missile defense for the US Navy and at least $378 million for GPS server maintained by Air Force/Space Force. |
| Extent to which the covered transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security | Major risk because of recent Chinese Cybersecurity and Intelligence Laws which can compel any Chinese company to collect, process, and transfer any data collected on their devices to the Chinese government |
| Whether the covered transaction is likely to have the effect of creating any new cybersecurity vulnerabilities in the United States or exacerbating existing cybersecurity vulnerabilities | The proliferation of Lenovo equipment in state and local government networks is a key concern because of sensitive personal information saved on the equipment as well as valuable corporate and financial information.[21] During COVID19 pandemic, there is increased risk from government and military employees unwittingly using Lenovo devices at home on insecure Wi-Fi networks |
| Whether the covered transaction is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States, including such activities designed to affect the outcome of any election for Federal office | Many US states collect, save, and process election information on Lenovo equipment |
| Whether the covered transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology that a United States business that is a party to the transaction possesses. | Lenovo is a national champion of the Chinese government and has executed China's go-to market strategy of acquiring key American technology brands. This is described in multiple USCC reports. |

Since Lenovo's 2014 acquisition, it has been subject to many security incidents, most notably the pre-installation of a malicious program on 750,134 laptops between 2014-2015. Called Visual Discovery, the program appeared to be a product recommendation and advertising engine, but it purveyed "man-in-the-middle" attacks which could break the user's secure connection with certain websites and exposes the user's sensitive, personal, and financial information to attackers. Lenovo settled charges from the Federal Trade Commission and 32 state attorneys general for $3.5 million in 2018.[22] Other incidents have included the installation of spyware on its laptops and smartphones[23,24,25] malware triggered from the

[21] Layton, Roslyn. China Tech Threat, 2020, *Stealing From States: China's Power Play in IT Contracts*

[22] "FTC Gives Final Approval to Lenovo Settlement." *Federal Trade Commission*, 2 Jan. 2018

"Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software That Compromised Security of Its Computers." *State of California Department of Justice*, 5 Sept. 2017

[23] Phillip, Joshua. "Spy Software Found Preinstalled on Lenovo, Huawei, and Xiaomi Smartphones." *The Epoch Times*, 9 Sept. 2015

[24] "SmartPhone Malware Found on Popular Brands ." Ophtek, 20 Oct. 2015

[25] Osborne, Charlie. "Lenovo Begs Users to Uninstall Accelerator App in the Name of Security." *ZD Net*, 2 June 2016

running on enterprise security programs[26,27]; Data mining software found on devices which collects/transmits sensitive user data without consent[28]; weak security which compromises login-in credentials and fingerprints[29]; the continued sending of user location to an unknown server in China[30]; and the breach of 36 terabytes of data from a severe vulnerability[31]. The National Vulnerabilities Database (NVD) list 325 Common Vulnerabilities and Exposures from Lenovo.[32]

The most common cyberattacks -- data breaches, phishing, and hacking--are driven primarily by organized crime and state-sponsored actors for financial and espionage reasons. Cyber attackers look for valuable personal and financial information; intellectual property and proprietary product information; corporate account information about key employees and customers; and corporate network access.

Given the pandemic, government and military employees have increasingly worked from home to access sensitive information, unwittingly with a vulnerable device connected to Wi-Fi, a useable but insecure network. Individuals, having endured extensive isolation during the pandemic, are further vulnerable to phishing and social engineering attacks as well as hacking as they increasingly multitask.

## MOVING FORWARD: MITIGATING EXISTING MERGERS

CFIUS has a broad range of tools which run the gamut from transparency remedies such as disclosures and audits; mitigation such as spinning off sensitive parts of the business and pledging to uphold strict protocols; to the outright blocking of the transaction, and even unwinding of earlier consummated transactions. To ensure compliance, CFIUS can impose significant fines (e.g. in the millions of dollars). CFIUS rulings have been challenged in court in the past, noting the "due process clause" of the Constitution which requires that affected parties be informed and be given access to the relevant evidence on which the decision was made.

The 2018 FIRRMA legislation updated the rules to CFIUS to improve due process. The key challenge for TikTok was that it pursued the merger without first informing CFIUS, an action which can automatically lead to CFIUS review. It is less likely that CFIUS would revisit Lenovo today, as it approved earlier acquisitions, albeit with less stringent conditions. The unwinding of mergers typically happens if the parties did not first inform CFIUS and if there is a security threat. In the Lenovo case, the five-year mitigation window for IBM's government accounts has passed, and resources are already committed to

[26] Patrizio, A. (2016, May 9). Lenovo software has a major security risk. *Network World*

[27] George, A. (2019, August 26). Your Lenovo laptop may have a serious security flaw. *Digital Trends*

[28] Wiggers, K. (2017, August 1). How to keep yourself safe from Chinese spyware on budget Android phones. *Digital Trends*

[29] Coppock, M. (2018, January 30). Lenovo fingerprint scanner software is broken, update it today. *Digital Trends*

[30] Whittaker, Z. (2019, February 11). Lenovo Watch X was Riddled With Security Bugs, Researcher Says. *Tech Crunch*

[31] Winder, D. (2019, July 18). Lenovo Confirms 36TB Data Leak Security Vulnerability. *Forbes*

[32] "National Vulnerability Database." National Institute of Standards and Technology

rip and replace the servers so they do not fall into Lenovo's hands. However, threats to privacy and security remain requiring that mitigation be taken by other government agencies and consumers themselves.

Many federal statues restrict federal funding for specific products and services, notably Huawei. However, these statutes should be strengthened and clarified to reflect that cybersecurity and informational privacy risk extends to any firm owned or affiliated by the Chinese government. The Federal Communications Commission (FCC) has the authority to restrict the operation of communications networks devices which pose security risks. State and local governments should take greater scrutiny to the selection and use of such equipment in their networks.

## CONCLUSION

The world is increasingly globalized, and foreign actors seek to access strategic US technology through a variety of transactions. While most foreign investment is mutually beneficial and undertaken by allies, there some transactions which require scrutiny. Investments from China in the US has tripled in recent years and is focused on acquiring strategic assets from US firms. Fortunately, Congress has updated CFIUS with greater role and resources to screen for national security implications of foreign investments in the US economy. CFIUS' role is to stop the enablement of foreign actors which would imperil national security. It operates on a basic principle of prevention, not to allow malicious foreign actors to acquire valuable US firms and technologies in the first place. While CFIUS might not be able to undo misguided mergers in the past, it better equipped to mitigate and prevent them in the future.