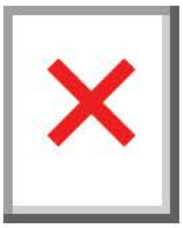
From: USDOJ-Office of Public Affairs
Subject: DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY DELIVERS REMARKS AT THE FIFTH NATIONAL CONFERENCE ON CFIUS AND TEAM TELECOM
To: Morrissey, Brian (OAG)
Sent: April 24, 2019 4:19 PM (UTC-04:00)



FOR IMMEDIATE RELEASE
WEDNESDAY, APRIL 24, 2019

DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY DELIVERS REMARKS AT THE FIFTH NATIONAL CONFERENCE ON CFIUS AND TEAM TELECOM

Washington, D.C.

Remarks as prepared for delivery

Good morning, and thank you for the invitation to return to this forum. This conference is one of the few devoted to national security reviews of foreign investment. It's a unique opportunity for us in the government to talk to the private sector about the threats we see and the approaches we are taking to address them, and to hear your concerns and questions in response. The dialogue that results helps us do a better job. So thank you for being here today.

As you know, the foreign investment and telecommunications landscape is rapidly changing, because of technological advancements, legal reforms, and changes in policy. There's a lot to discuss in the next two days, especially because of changes in the statutory authority underpinning CFIUS. But before I turn to foreign investment and telecom security work, specifically, I want to take a step back and describe the larger context for that work at the Justice Department. I want to give you a sense of how we view certain threats related to China, which, I hope, will give you a better sense of our perspective on foreign investment reviews that concern our areas of expertise and equities. Then I will turn to the Foreign Investment Risk Review Modernization Act (FIRRMA) and how I expect it to improve how the Department conducts its reviews, better tailoring our efforts to meet modern threats and allocating resources to the most complex cases.

I. The China Initiative

As you may be aware, in November 2018, then-Attorney General Sessions announced a "China Initiative" at the Justice Department. Attorney General Barr has indicated he supports it, and the Initiative continues under his leadership of the Department.

Why has the Justice Department started a China Initiative? Because we see increasing threats to national security from Chinese state actors, across a range of vectors. Broadly speaking, the China Initiative aims to raise awareness of those threats, to focus the Department's resources in confronting them, and to improve our response, particularly to newer challenges.

The Department's prosecutors and other lawyers have choices to make in deploying limited resources, opening and prosecuting cases, in our foreign investment reviews, and so forth. When the Attorney General announces that certain types of cases, and certain threats, are priorities, it matters to our decisions. And I hope it matters to the private sector, as well.

A. The Threats

So what do I mean by "threats" from China? Let me begin with China's industrial policy. As reports by the U.S. Trade Representative (USTR) and others have laid out, the Chinese government regards technology development as integral to its economic development and has set out an ambitious agenda to become a global leader in a wide range of technologies. More than 100 five-year plans, science and technology development plans, and sectoral plans have issued over the last decade, all in pursuit of that objective.

To take one example, in 2015, China's State Council released the "Made in China 2025 Notice," a ten-year plan for targeting ten strategic manufacturing industries for promotion and development: (1) next generation information technology; (2) robotics and automated machine tools; (3) aircraft and aircraft components (aerospace); (4) maritime vessels and marine engineering equipment; (5) advanced rail equipment; (6) clean energy vehicles; (7) electrical generation and transmission equipment; (8) agricultural machinery and equipment; (9) new materials; and (10) biotechnology. The program leverages the Chinese government's power and central role in economic planning to alter competitive dynamics in global markets and acquire technologies in these industries. To achieve the program's benchmarks, China aims to localize research and development, control segments of global supply chains, prioritize domestic production of technology, and capture global market share across these industries.

In so doing, China has committed to pursuing an "innovation-driven" development strategy. But if that's all the policy amounted to, we would have nothing to complain about. No one faults a nation for aspiring to self-sufficiency in strategically important industries.

The problem is not that China is working to master critical technologies, or even that it is competing with the United States, but rather the means by which it is doing so.

"Made in China 2025" is as much a roadmap to theft as it is guidance to innovate. Since the plan was announced in 2015, the Justice Department has charged Chinese individuals and entities with trade secret theft implicating at least eight of the ten sectors. Over a longer time period, since 2011, more than 90 percent of the Department's economic espionage prosecutions (*i.e.*, cases alleging trade secret theft by or to benefit a foreign state) involve China, and more than two-thirds of all federal trade secret theft cases during that period have had at least a geographical nexus to China.

Some of those cases demonstrate that China is using its intelligence services and their tradecraft to target our private sector's intellectual property. In the space of two months last year, the Department announced three cases alleging crimes by the same arm of the Chinese intelligence services, the Jiangsu Ministry of State Security, also known as the "JSSD."

- In October, the Department announced the unprecedented extradition of a Chinese intelligence officer accused of seeking technical information about jet aircraft engines from leading aviation companies in the United States and elsewhere. According to the indictment, while concealing his true employment, he recruited the companies' aviation experts to travel to China under the guise of participating in university lectures and a nongovernmental "exchange" of ideas with academics. In fact, the experts' audience worked for the Chinese government.

- In another case unsealed that month, two JSSD officers were charged with managing a team of hackers to conduct computer intrusions against at least a dozen companies, a number of whom had information related to a turbofan engine used in commercial jetliners. A Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft at or about the same time, and it could have saved substantial research and development expenses by exploiting that stolen data. The defendants are charged with co-opting at least two Chinese nationals employed by one of the victims, who infected the company's network with malware and warned the JSSD when law enforcement appeared to be investigating.
- Finally, in September, the Department charged a U.S. Army reservist, who is also a Chinese national, with acting as a source for a JSSD intelligence officer. According to the complaint in that case, the Chinese intelligence officer prompted his source (the defendant) to obtain background information on eight individuals, including other Chinese nationals who were working as engineers and scientists in the United States (some for defense contractors) for the purpose of recruiting them.

A fourth case, unsealed in December, charged two individuals with working in association with a different bureau of the Ministry of State Security to conduct a global campaign of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs) (companies that remotely manage the information technology infrastructure of businesses and governments around the world), more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies.

The group they worked for, commonly known as APT 10, targeted a diverse array of industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production.

These techniques—covertly recruiting assets, hacking into networks—are not themselves shocking in the context of traditional espionage, the targeting of one government's secrets by another. But this is not traditional: the concerted efforts and resources of a determined nation-state target our private sector.

Moreover, these actions are contrary to both the spirit and, in some cases, the letter, of China's 2015 commitment to the international community not to steal trade secrets and other confidential business information through computer hacking "with the intent of providing competitive advantages to [its] companies or commercial sectors."

To be sure, there are trade secret cases where we cannot prove beyond a reasonable doubt that the Chinese government itself directed the theft. One example was the conviction of a Chinese company—the Sinovel Wind Group Company—for stealing wind turbine technology from a U.S. company resulting in the victim losing more than $1 billion in shareholder equity and almost 700 jobs, more than half of its global workforce. Another was the conviction of a Chinese scientist for theft of genetically modified rice seeds with biopharmaceutical applications, providing a direct economic benefit to the Chinese crop institute that was the intended recipient of the seeds. But although we could not prove in court that these thefts were directed by the Chinese government, they are in perfect consonance with the Chinese government's economic policy. And the absence of meaningful protections for intellectual property in China, the paucity of cooperation with any requests for assistance in investigating these cases, the plethora of state sponsored enterprises, and the authoritarian control exercised by the Communist Party—all of which create an environment where such thefts are tolerated, if not rewarded—amply justify the conclusion that the Chinese government is in some sense responsible for those thefts, too.

B. The Rule of Law

This brings me to another aspect of the threat we face from China: its failure to honor its commitments or to respect the rule of law and legal process more generally.

When a Chinese firm or individual violates American law, requests by us for documents and interviews go unanswered for years, and commitments to cooperate go unfulfilled. In 2015, China and the United States agreed to cooperate with requests to investigate computer crime, collect electronic evidence, and

mitigate malicious cyber activity emanating from their respective territories. Yet in 2017, when the Department invoked that commitment to request assistance in connection with an investigation of a purported Internet security firm for trade secret theft, we received no meaningful response.

Since 2001, the United States and China have had a Mutual Legal Assistance Agreement. The Agreement creates an obligation, after one country makes a request to the other, to provide evidence gathering and other assistance "in investigations, in prosecutions, and in proceedings related to criminal matters." Over the past 10 years, however, China has rarely produced bank or similar transactional records pursuant to multiple MLA requests. And in the minority of cases where it produced records, they were incomplete, untimely, or inadmissible. And when we exercise our authorities as federal prosecutors to compel businesses located here to produce records, the Chinese government threatens them not to comply, on pain of sanctions under their laws.

We do not have an extradition treaty with China, but China by and large will not prosecute its nationals who violate our laws. Even requests to serve the charges on the defendants, so that they may answer them in our courts under due process of law, are rebuffed. For years, we struggled to hold the Pangang Group accountable on charges that it conspired with a former employee of DuPont and others to steal the trade secrets that enable the company to make Titanium Dioxide, a compound used to color everything from house paint to food "white." The Chinese government refused repeated requests to serve the charges on the Pangang entities. Because of that recalcitrance, the Department persuaded the Supreme Court to change the applicable rule of criminal procedure to permit additional means of giving notice of charges, and federal courts have now held that Pangang Group was served. It is scheduled to stand trial early next year.

Even where we or our law enforcement partners obtain custody of Chinese nationals, China appears to detain foreign citizens as a means of retaliating or inflicting political pressure. In 2014, Canadian authorities arrested a Chinese national named Su Bin at the request of the United States. We sought his extradition for hacking-related offenses and the theft of sensitive military and export-controlled data that was sent to China.

In an apparent act of reprisal, Chinese authorities apprehended a Canadian couple who had lived in China for 30 years without incident. They were accused of spying and threatened with execution. The wife was detained for six months before being released on conditions. The husband did not meet with a lawyer for almost a year. He was held for more than two years.

On the other hand, when China seeks to track down its nationals accused of political or corruption crimes, they have refused to work with U.S. authorities to bring them to justice. Instead, it has been known to send agents known as "Fox Hunt" teams to the United States and elsewhere to "persuade" their fugitives to return to China. The squads enter foreign countries under false pretenses, track down their fugitives and deploy intimidation tactics to force them to return to China.

C. Our Strategy

To respond to these threats, the China Initiative establishes a number of goals and priorities.

Investigating and prosecuting economic espionage and other federal crimes will remain at the heart of our work. We will ensure that these investigations and prosecutions are adequately resourced and prioritized. And we will continue to work with a growing list of likeminded nations to do so. But as important as they are, we must broaden our approach. Here are three other prongs to our strategy.

First, criminal prosecution alone is not enough to remediate the harm caused by theft or to deter future thieves. That's why we are looking for ways to use our tools to support those of our federal partners, including economic tools available to the Departments of the Treasury and Commerce and the U.S. Trade Representative, diplomacy by the State Department, and engagement by the military and intelligence community.

A recent case is a great example of this approach. Until recently, China did not possess the technology needed to manufacture a basic kind of computer memory, known as dynamic random-access memory ("DRAM"). The worldwide market for DRAM is worth nearly $100 billion, and an American company in Idaho, Micron, controls about 20 to 25 percent of that market. In 2016, however, the Chinese Central Government and the State Council publicly identified the development of DRAM as a national economic priority and stood up a company to mass produce it.

priority and stood up a company to mass produce it.

How did they set out to meet that goal? According to an indictment unsealed in San Francisco in November, a Taiwan competitor poached three of Micron's employees, who stole trade secrets about DRAM worth up to $8.75 billion from Micron. The Taiwan company then partnered with a Chinese state-owned company to manufacture the memory. And in a galling twist, when Micron sought redress through the courts, the Chinese company sued *Micron* for infringing its patents.

Our goal was not just to hold the thieves accountable: we want to ensure that Micron does not have to compete against its own intellectual property. So, in addition to the criminal indictment, we civilly sued both the Chinese and Taiwan competitors, seeking an injunction that would bar the importation of any products based on the stolen technology into the United States. And days before our charges were announced, the Commerce Department placed the Chinese state-owned enterprise on the Entity List, which should prevent it from acquiring the goods and services required to manufacture DRAM based on the stolen trade secrets. Through these actions, we have sought to deprive the foreign companies of unjust enrichment, mitigating harm to Micron and, we believe, deterring similar conduct by others.

Second, the best strategy empowers American businesses and the private sector to defend themselves in the first place. That is why we are equipping our U.S. Attorneys around the country with the information they need to speak about these threats to companies and others in their jurisdictions, raising awareness and developing the relationships of trust and cooperation that lead both to effective prevention and to partnerships with law enforcement in responding to incidents.

That is also why we need to develop enforcement strategies that target non-traditional threats in unique, sometimes sensitive contexts. I am speaking here of non-traditional collectors, including researchers in labs, universities, and the defense industrial base, some of whom may have undisclosed ties to Chinese institutions and conflicted loyalties based on the expectation of reward through Talent Plans and other PRC incentive programs. I am also thinking of covert efforts to influence public opinion and policy, by leveraging student groups on campus that have ties to the Chinese consulate, or American businessmen with interests in China. Outreach and education will be critical to countering conduct that is covert, corrupt, or coercive, but for which criminal tools may not be the best, first choice.

Third, we must better secure our telecommunications networks from supply chain threats and guard against other national security threats through foreign investment. It is this aspect of the China Initiative that I want to spend the balance of my time on.

All too often in this context, the security of a product or service, or the threat from a company that sells it, is debated as if the test is binary: whether there is proof, a "smoking gun," so to speak, that the company in question is currently breaking the law by, say, conducting illicit surveillance. But whether a company has a culture that promotes theft, dishonesty, or obstruction of justice is just as relevant, because it tells you how the company will behave when it suits its interests.

Our cases show that the Chinese government will use the employees of Chinese companies doing business here to engage in illegal activity. A week ago [April 17], a former airline ticket counter agent pleaded guilty to acting as an agent of the Chinese government, without notification to the Attorney General, by working at the direction and control of military officers assigned to China's Permanent Mission to the United Nations. During her employment at JFK with a Chinese Air Carrier, she accepted packages from PRC military officers, and placed those packages aboard Air Carrier flights to China as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. She encouraged other Air Carrier employees to assist the military officers, telling them that, because the Air Carrier was a Chinese company, their primary loyalty should be to China. But covertly doing the Chinese military's bidding on U.S. soil is a crime, and the defendant and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight. Her actions violated TSA regulations requiring checked baggage be accepted only from ticketed passengers.

While there is a presumption of innocence in the criminal context, we are here today as risk managers, not criminal lawyers. We must gauge the likelihood that a company or individual will want to (or be coerced to)—and can—exploit a vulnerability, and how dire (or not) the consequences of that action are likely to be. And then we must evaluate whether there is a reliable way to lower the overall risk of those eventualities to tolerable levels. It's more art than science, to be sure, but in making our assessments, we

should consider all of the relevant evidence, including the implications of doing business in an

should consider all of the relevant evidence, including the implications of doing business in an authoritarian state.

In my remarks so far, I have made the case that the Chinese government has the stated motive and intent to dominate certain, critical technologies. I have also given you examples that the PRC is using a combination of intelligence services and other hybrid techniques to target our companies to that end or exploit their presence here. And I have described Chinese unwillingness to adhere to its stated commitments or play by reciprocal rules. Added together, these are reasons for concern that may add up to an intolerable risk in the context of particular transactions.

Last July, the Administration recommended that the Federal Communications Commission deny an application by the indirect U.S. subsidiary of China Mobile Communications Corporation (a Chinese state-owned enterprise and the world's largest telecom carrier) for a license to offer international telecommunications services in the United States, under Section 214 of the Communications Act of 1934. The Justice Department led the national security and law enforcement review of the application, and the Executive Branch's recommendation highlights the risks to U.S. law enforcement and national security from granting the indirect subsidiary of a Chinese state-owned enterprise the status of a common carrier provider of telecommunications services. Such a status would give China Mobile access to trusted, peering relationships with American carriers.

In evaluating whether the China Mobile application was in the public interest, the Department considered a number of factors, including whether the applicant's planned operations would provide opportunities to undermine the reliability and stability of our communications infrastructure, including by rendering it vulnerable to exploitation, manipulation, attack, sabotage, or covert monitoring; to enable economic espionage; and to undermine authorized law enforcement and national security missions. As the recommendation puts it, in light of those factors, "because China Mobile is subject to exploitation, influence, and control by the Chinese government, granting China Mobile's [application] in the current national security environment, would pose substantial and unacceptable national security and law enforcement risks."

Last week, we were gratified to learn that FCC Chairman Ajit Pai announced that, in his view, "it is clear that China Mobile's application . . . raises substantial and serious national security and law enforcement risks" and that "approving it would [not] be in the public interest." He urged his fellow commissioners to reject its application at their May meeting.

Cases like China Mobile have brought home to the Department how important our foreign investment review work is to protecting our equities in law enforcement, counterintelligence, and telecom security. That is why, during the first two years of this Administration, we co-led more CFIUS reviews than in the five years before that, combined. That is why we have renamed the staff that conducts these reviews to be a "Section," and reorganized its management structure, to match other operational components of NSD. And that is why the President's proposed budget for the Department would significantly increase the staff and other resources devoted to this work.

II. FIRRMA

In doing so, we are positioning ourselves to be ready to do our part in implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). We are already working closely with the Department of the Treasury to implement the newly launched pilot program under the statute and to develop regulations to implement the Committee's expanded authority.

As this room already knows, FIRRMA represents the most significant reform of the CFIUS process in more than a decade. The Department was pleased to support the act, which adapts CFIUS to address current threats. Most significantly, in my view, it expands the Committee's authority to address emerging national security risks that fall outside foreign control thresholds, such as minority investments that give access to sensitive information or technology, or any deal structured to circumvent CFIUS review.

But FIRRMA is not just about expanding the government's power. I believe the legislation reflects a commitment to increased transparency, predictability, and efficiency in the CFIUS process, a commitment we share. More specifically:

1. The new declaration process mandates that companies contemplating qualifying transactions file

1. The new declaration process mandates that companies contemplating qualifying transactions file short notifications before consummating a transaction, but this "light filing" requires much less information than a voluntary notification, and it allows the Committee to clear low risk transactions much faster (providing certainty to the parties where appropriate) and to identify significant national security issues in other cases before closing.
2. FIRRMA extends the initial review period by 15 days, but even that small increase should allow the Committee to clear more transactions in review and to reduce the need to re-file cases.
3. By specifying that any judicial review occur before the Court of Appeals for the D.C. Circuit, the legislation shortens the time required for judicial review and ensures that a consistent body of precedent develops in one court with extensive experience reviewing administrative decisions.
4. And by giving CFIUS agencies specialized authority to hire additional staff, it ensures that we can manage the additional CFIUS filings that we expect.

In these ways, FIRRMA reflects our longstanding open investment policy, makes the United States an attractive location for foreign investors, and applies neutrally to investment from any country.

By contrast, and as USTR has highlighted in its Section 301 reports, U.S. companies trying to enter the Chinese market must navigate foreign ownership restrictions, joint venture requirements, discriminatory licensing regimes, and vague and discretionary administrative approval processes that allow the Chinese government to pressure them to transfer their technology as a condition of market access.

In seeking to protect against national security risk, we must remember that free enterprise, market incentives, and the exchange of capital, people, and ideas across borders have been critical ingredients to our economic success. The ultimate goal of our foreign investment reviews is to preserve the framework of private choices and freedom that has made our companies and innovations the envy of the world.

Along those lines, we must also work to reform the *ad hoc* process by which the Executive Branch advises the FCC on license applications, known as Team Telecom. Although I am pleased with the ultimate recommendation in the China Mobile matter, which sets an important precedent, we must explore ways to make this process more efficient and expedient, so that the Executive Branch never again takes nearly seven years to make a recommendation.

Conclusion

Despite the threats and challenges we face, last year was a tremendous one for American innovation. In 2018, U.S. companies obtained 142,000 new U.S. utility grant patents out of the more than 308,000 patents that the U.S. Patent and Trademark Office approved. Six of the top 10 U.S. patent recipients were U.S. corporations. As of 2016, industries that rely heavily on intellectual property supported at least 45 million U.S. jobs and contributed more than $6 trillion dollars to, or 38.2 percent of, U.S. gross domestic product.

Last year's headlines offers examples of inventions and advances that are truly miraculous:

- In January, a Massachusetts company introduced the first commercial version of its four-legged, dog-like robot at the Consumer Electronics Show in Las Vegas. This robot can already run, jump, dance, and open doors. The commercial version is being tested for use in construction, work place inspection, and physical security, to name just a few potential uses.
- In April, a California company announced its next generation drone, capable of flying at a speed of up to 80 mph for a range of up to 99 miles round trip while carrying up to 3.9 lbs. Among other uses, drones like this can carry shipments of donated blood or other specialized medical supplies across difficult terrain with few paved roads.
- In June, a Massachusetts medical device company conducted a groundbreaking two week study of their Closed-Loop insulin delivery system. The system is essentially a bionic pancreas, one of a handful of FDA-approved technologies that combines both a glucose monitor and insulin pump to almost entirely automate blood sugar control in type 1 diabetics. The study showed that in normal living conditions Type 1 diabetics could better control blood sugar and reduce incidences of hypoglycemia with the closed loop system; no finger pricks required.
- A U.S. automaker released a luxury sedan with its new semiautonomous, hands-free driver assistance technology. This technology relies upon LiDAR (or laser sensors that work like radar)

assistance technology. This technology relies upon LIDAR (or laser sensors that work like radar) mapping, in-car cameras, radar sensors, and GPS to detect the road ahead, control speed, and maintain lane position while allowing the driver to travel without touching the wheel or pedals. You still need to pay attention to the road, however, and if the driver begins to nod off or get distracted, the vehicle will alert the driver through a series of escalating vibrations and chimes. This automaker has announced plans to install the semiautonomous technology in all new vehicles by 2020, moving us one-step closer to safe, self-driving vehicles on U.S. road.

- Finally, in December 2018, a California company conducted a test flight of a manned, suborbital plane designed for space tourism. The flight, which was the fastest and highest commercial test flight to-date, reached a peak altitude of roughly 51 miles above the Earth's surface. It was the first time a commercial vehicle designed for tourism entered outer space.

I believe that, if we get it right---if we balance tailored authorities and a focus on national security with respect for free markets---we will continue to see unparalleled innovations like these in the United States, fueled in no small part by foreign investment. And in the coming year, I look forward to working with you to strike that balance.

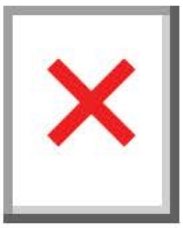
# # #

NSD

19-416

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY DELIVERS REMARKS AT THE FIFTH NATIONAL CONFERENCE ON CFIUS AND TEAM TELECOM
To: Watson, Theresa (OAG)
Sent: April 24, 2019 4:19 PM (UTC-04:00)



FOR IMMEDIATE RELEASE
WEDNESDAY, APRIL 24, 2019

DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY DELIVERS REMARKS AT THE FIFTH NATIONAL CONFERENCE ON CFIUS AND TEAM TELECOM

Washington, D.C.

Remarks as prepared for delivery

Good morning, and thank you for the invitation to return to this forum. This conference is one of the few devoted to national security reviews of foreign investment. It's a unique opportunity for us in the government to talk to the private sector about the threats we see and the approaches we are taking to address them, and to hear your concerns and questions in response. The dialogue that results helps us do a better job. So thank you for being here today.

As you know, the foreign investment and telecommunications landscape is rapidly changing, because of technological advancements, legal reforms, and changes in policy. There's a lot to discuss in the next two days, especially because of changes in the statutory authority underpinning CFIUS. But before I turn to foreign investment and telecom security work, specifically, I want to take a step back and describe the larger context for that work at the Justice Department. I want to give you a sense of how we view certain threats related to China, which, I hope, will give you a better sense of our perspective on foreign investment reviews that concern our areas of expertise and equities. Then I will turn to the Foreign Investment Risk Review Modernization Act (FIRRMA) and how I expect it to improve how the Department conducts its reviews, better tailoring our efforts to meet modern threats and allocating resources to the most complex cases.

I. The China Initiative

As you may be aware, in November 2018, then-Attorney General Sessions announced a "China Initiative" at the Justice Department. Attorney General Barr has indicated he supports it, and the Initiative continues under his leadership of the Department.

Why has the Justice Department started a China Initiative? Because we see increasing threats to national security from Chinese state actors, across a range of vectors. Broadly speaking, the China Initiative aims to raise awareness of those threats, to focus the Department's resources in confronting them, and to improve our response, particularly to newer challenges.

The Department's prosecutors and other lawyers have choices to make in deploying limited resources, opening and prosecuting cases, in our foreign investment reviews, and so forth. When the Attorney General announces that certain types of cases, and certain threats, are priorities, it matters to our decisions. And I hope it matters to the private sector, as well.

A. The Threats

So what do I mean by "threats" from China? Let me begin with China's industrial policy. As reports by the U.S. Trade Representative (USTR) and others have laid out, the Chinese government regards technology development as integral to its economic development and has set out an ambitious agenda to become a global leader in a wide range of technologies. More than 100 five-year plans, science and technology development plans, and sectoral plans have issued over the last decade, all in pursuit of that objective.

To take one example, in 2015, China's State Council released the "Made in China 2025 Notice," a ten-year plan for targeting ten strategic manufacturing industries for promotion and development: (1) next generation information technology; (2) robotics and automated machine tools; (3) aircraft and aircraft components (aerospace); (4) maritime vessels and marine engineering equipment; (5) advanced rail equipment; (6) clean energy vehicles; (7) electrical generation and transmission equipment; (8) agricultural machinery and equipment; (9) new materials; and (10) biotechnology. The program leverages the Chinese government's power and central role in economic planning to alter competitive dynamics in global markets and acquire technologies in these industries. To achieve the program's benchmarks, China aims to localize research and development, control segments of global supply chains, prioritize domestic production of technology, and capture global market share across these industries.

In so doing, China has committed to pursuing an "innovation-driven" development strategy. But if that's all the policy amounted to, we would have nothing to complain about. No one faults a nation for aspiring to self-sufficiency in strategically important industries.

The problem is not that China is working to master critical technologies, or even that it is competing with the United States, but rather the means by which it is doing so.

"Made in China 2025" is as much a roadmap to theft as it is guidance to innovate. Since the plan was announced in 2015, the Justice Department has charged Chinese individuals and entities with trade secret theft implicating at least eight of the ten sectors. Over a longer time period, since 2011, more than 90 percent of the Department's economic espionage prosecutions (*i.e.*, cases alleging trade secret theft by or to benefit a foreign state) involve China, and more than two-thirds of all federal trade secret theft cases during that period have had at least a geographical nexus to China.

Some of those cases demonstrate that China is using its intelligence services and their tradecraft to target our private sector's intellectual property. In the space of two months last year, the Department announced three cases alleging crimes by the same arm of the Chinese intelligence services, the Jiangsu Ministry of State Security, also known as the "JSSD."

- In October, the Department announced the unprecedented extradition of a Chinese intelligence officer accused of seeking technical information about jet aircraft engines from leading aviation companies in the United States and elsewhere. According to the indictment, while concealing his true employment, he recruited the companies' aviation experts to travel to China under the guise of participating in university lectures and a nongovernmental "exchange" of ideas with academics. In fact, the experts' audience worked for the Chinese government.

- In another case unsealed that month, two JSSD officers were charged with managing a team of hackers to conduct computer intrusions against at least a dozen companies, a number of whom had information related to a turbofan engine used in commercial jetliners. A Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft at or about the same time, and it could have saved substantial research and development expenses by exploiting that stolen data. The defendants are charged with co-opting at least two Chinese nationals employed by one of the victims, who infected the company's network with malware and warned the JSSD when law enforcement appeared to be investigating.
- Finally, in September, the Department charged a U.S. Army reservist, who is also a Chinese national, with acting as a source for a JSSD intelligence officer. According to the complaint in that case, the Chinese intelligence officer prompted his source (the defendant) to obtain background information on eight individuals, including other Chinese nationals who were working as engineers and scientists in the United States (some for defense contractors) for the purpose of recruiting them.

A fourth case, unsealed in December, charged two individuals with working in association with a different bureau of the Ministry of State Security to conduct a global campaign of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs) (companies that remotely manage the information technology infrastructure of businesses and governments around the world), more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies.

The group they worked for, commonly known as APT 10, targeted a diverse array of industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production.

These techniques—covertly recruiting assets, hacking into networks—are not themselves shocking in the context of traditional espionage, the targeting of one government's secrets by another. But this is not traditional: the concerted efforts and resources of a determined nation-state target our private sector.

Moreover, these actions are contrary to both the spirit and, in some cases, the letter, of China's 2015 commitment to the international community not to steal trade secrets and other confidential business information through computer hacking "with the intent of providing competitive advantages to [its] companies or commercial sectors."

To be sure, there are trade secret cases where we cannot prove beyond a reasonable doubt that the Chinese government itself directed the theft. One example was the conviction of a Chinese company—the Sinovel Wind Group Company—for stealing wind turbine technology from a U.S. company resulting in the victim losing more than $1 billion in shareholder equity and almost 700 jobs, more than half of its global workforce. Another was the conviction of a Chinese scientist for theft of genetically modified rice seeds with biopharmaceutical applications, providing a direct economic benefit to the Chinese crop institute that was the intended recipient of the seeds. But although we could not prove in court that these thefts were directed by the Chinese government, they are in perfect consonance with the Chinese government's economic policy. And the absence of meaningful protections for intellectual property in China, the paucity of cooperation with any requests for assistance in investigating these cases, the plethora of state sponsored enterprises, and the authoritarian control exercised by the Communist Party—all of which create an environment where such thefts are tolerated, if not rewarded—amply justify the conclusion that the Chinese government is in some sense responsible for those thefts, too.

B. The Rule of Law

This brings me to another aspect of the threat we face from China: its failure to honor its commitments or to respect the rule of law and legal process more generally.

When a Chinese firm or individual violates American law, requests by us for documents and interviews go unanswered for years, and commitments to cooperate go unfulfilled. In 2015, China and the United States agreed to cooperate with requests to investigate computer crime, collect electronic evidence, and

mitigate malicious cyber activity emanating from their respective territories. Yet in 2017, when the Department invoked that commitment to request assistance in connection with an investigation of a purported Internet security firm for trade secret theft, we received no meaningful response.

Since 2001, the United States and China have had a Mutual Legal Assistance Agreement. The Agreement creates an obligation, after one country makes a request to the other, to provide evidence gathering and other assistance "in investigations, in prosecutions, and in proceedings related to criminal matters." Over the past 10 years, however, China has rarely produced bank or similar transactional records pursuant to multiple MLA requests. And in the minority of cases where it produced records, they were incomplete, untimely, or inadmissible. And when we exercise our authorities as federal prosecutors to compel businesses located here to produce records, the Chinese government threatens them not to comply, on pain of sanctions under their laws.

We do not have an extradition treaty with China, but China by and large will not prosecute its nationals who violate our laws. Even requests to serve the charges on the defendants, so that they may answer them in our courts under due process of law, are rebuffed. For years, we struggled to hold the Pangang Group accountable on charges that it conspired with a former employee of DuPont and others to steal the trade secrets that enable the company to make Titanium Dioxide, a compound used to color everything from house paint to food "white." The Chinese government refused repeated requests to serve the charges on the Pangang entities. Because of that recalcitrance, the Department persuaded the Supreme Court to change the applicable rule of criminal procedure to permit additional means of giving notice of charges, and federal courts have now held that Pangang Group was served. It is scheduled to stand trial early next year.

Even where we or our law enforcement partners obtain custody of Chinese nationals, China appears to detain foreign citizens as a means of retaliating or inflicting political pressure. In 2014, Canadian authorities arrested a Chinese national named Su Bin at the request of the United States. We sought his extradition for hacking-related offenses and the theft of sensitive military and export-controlled data that was sent to China.

In an apparent act of reprisal, Chinese authorities apprehended a Canadian couple who had lived in China for 30 years without incident. They were accused of spying and threatened with execution. The wife was detained for six months before being released on conditions. The husband did not meet with a lawyer for almost a year. He was held for more than two years.

On the other hand, when China seeks to track down its nationals accused of political or corruption crimes, they have refused to work with U.S. authorities to bring them to justice. Instead, it has been known to send agents known as "Fox Hunt" teams to the United States and elsewhere to "persuade" their fugitives to return to China. The squads enter foreign countries under false pretenses, track down their fugitives and deploy intimidation tactics to force them to return to China.

C. Our Strategy

To respond to these threats, the China Initiative establishes a number of goals and priorities.

Investigating and prosecuting economic espionage and other federal crimes will remain at the heart of our work. We will ensure that these investigations and prosecutions are adequately resourced and prioritized. And we will continue to work with a growing list of likeminded nations to do so. But as important as they are, we must broaden our approach. Here are three other prongs to our strategy.

First, criminal prosecution alone is not enough to remediate the harm caused by theft or to deter future thieves. That's why we are looking for ways to use our tools to support those of our federal partners, including economic tools available to the Departments of the Treasury and Commerce and the U.S. Trade Representative, diplomacy by the State Department, and engagement by the military and intelligence community.

A recent case is a great example of this approach. Until recently, China did not possess the technology needed to manufacture a basic kind of computer memory, known as dynamic random-access memory ("DRAM"). The worldwide market for DRAM is worth nearly $100 billion, and an American company in Idaho, Micron, controls about 20 to 25 percent of that market. In 2016, however, the Chinese Central Government and the State Council publicly identified the development of DRAM as a national economic priority and stood up a company to mass produce it.

priority and stood up a company to mass produce it.

How did they set out to meet that goal? According to an indictment unsealed in San Francisco in November, a Taiwan competitor poached three of Micron's employees, who stole trade secrets about DRAM worth up to $8.75 billion from Micron. The Taiwan company then partnered with a Chinese state-owned company to manufacture the memory. And in a galling twist, when Micron sought redress through the courts, the Chinese company sued *Micron* for infringing its patents.

Our goal was not just to hold the thieves accountable: we want to ensure that Micron does not have to compete against its own intellectual property. So, in addition to the criminal indictment, we civilly sued both the Chinese and Taiwan competitors, seeking an injunction that would bar the importation of any products based on the stolen technology into the United States. And days before our charges were announced, the Commerce Department placed the Chinese state-owned enterprise on the Entity List, which should prevent it from acquiring the goods and services required to manufacture DRAM based on the stolen trade secrets. Through these actions, we have sought to deprive the foreign companies of unjust enrichment, mitigating harm to Micron and, we believe, deterring similar conduct by others.

Second, the best strategy empowers American businesses and the private sector to defend themselves in the first place. That is why we are equipping our U.S. Attorneys around the country with the information they need to speak about these threats to companies and others in their jurisdictions, raising awareness and developing the relationships of trust and cooperation that lead both to effective prevention and to partnerships with law enforcement in responding to incidents.

That is also why we need to develop enforcement strategies that target non-traditional threats in unique, sometimes sensitive contexts. I am speaking here of non-traditional collectors, including researchers in labs, universities, and the defense industrial base, some of whom may have undisclosed ties to Chinese institutions and conflicted loyalties based on the expectation of reward through Talent Plans and other PRC incentive programs. I am also thinking of covert efforts to influence public opinion and policy, by leveraging student groups on campus that have ties to the Chinese consulate, or American businessmen with interests in China. Outreach and education will be critical to countering conduct that is covert, corrupt, or coercive, but for which criminal tools may not be the best, first choice.

Third, we must better secure our telecommunications networks from supply chain threats and guard against other national security threats through foreign investment. It is this aspect of the China Initiative that I want to spend the balance of my time on.

All too often in this context, the security of a product or service, or the threat from a company that sells it, is debated as if the test is binary: whether there is proof, a "smoking gun," so to speak, that the company in question is currently breaking the law by, say, conducting illicit surveillance. But whether a company has a culture that promotes theft, dishonesty, or obstruction of justice is just as relevant, because it tells you how the company will behave when it suits its interests.

Our cases show that the Chinese government will use the employees of Chinese companies doing business here to engage in illegal activity. A week ago [April 17], a former airline ticket counter agent pleaded guilty to acting as an agent of the Chinese government, without notification to the Attorney General, by working at the direction and control of military officers assigned to China's Permanent Mission to the United Nations. During her employment at JFK with a Chinese Air Carrier, she accepted packages from PRC military officers, and placed those packages aboard Air Carrier flights to China as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. She encouraged other Air Carrier employees to assist the military officers, telling them that, because the Air Carrier was a Chinese company, their primary loyalty should be to China. But covertly doing the Chinese military's bidding on U.S. soil is a crime, and the defendant and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight. Her actions violated TSA regulations requiring checked baggage be accepted only from ticketed passengers.

While there is a presumption of innocence in the criminal context, we are here today as risk managers, not criminal lawyers. We must gauge the likelihood that a company or individual will want to (or be coerced to)—and can—exploit a vulnerability, and how dire (or not) the consequences of that action are likely to be. And then we must evaluate whether there is a reliable way to lower the overall risk of those eventualities to tolerable levels. It's more art than science, to be sure, but in making our assessments, we

should consider all of the relevant evidence, including the implications of doing business in an

should consider all of the relevant evidence, including the implications of doing business in an authoritarian state.

In my remarks so far, I have made the case that the Chinese government has the stated motive and intent to dominate certain, critical technologies. I have also given you examples that the PRC is using a combination of intelligence services and other hybrid techniques to target our companies to that end or exploit their presence here. And I have described Chinese unwillingness to adhere to its stated commitments or play by reciprocal rules. Added together, these are reasons for concern that may add up to an intolerable risk in the context of particular transactions.

Last July, the Administration recommended that the Federal Communications Commission deny an application by the indirect U.S. subsidiary of China Mobile Communications Corporation (a Chinese state-owned enterprise and the world's largest telecom carrier) for a license to offer international telecommunications services in the United States, under Section 214 of the Communications Act of 1934. The Justice Department led the national security and law enforcement review of the application, and the Executive Branch's recommendation highlights the risks to U.S. law enforcement and national security from granting the indirect subsidiary of a Chinese state-owned enterprise the status of a common carrier provider of telecommunications services. Such a status would give China Mobile access to trusted, peering relationships with American carriers.

In evaluating whether the China Mobile application was in the public interest, the Department considered a number of factors, including whether the applicant's planned operations would provide opportunities to undermine the reliability and stability of our communications infrastructure, including by rendering it vulnerable to exploitation, manipulation, attack, sabotage, or covert monitoring; to enable economic espionage; and to undermine authorized law enforcement and national security missions. As the recommendation puts it, in light of those factors, "because China Mobile is subject to exploitation, influence, and control by the Chinese government, granting China Mobile's [application] in the current national security environment, would pose substantial and unacceptable national security and law enforcement risks."

Last week, we were gratified to learn that FCC Chairman Ajit Pai announced that, in his view, "it is clear that China Mobile's application . . . raises substantial and serious national security and law enforcement risks" and that "approving it would [not] be in the public interest." He urged his fellow commissioners to reject its application at their May meeting.

Cases like China Mobile have brought home to the Department how important our foreign investment review work is to protecting our equities in law enforcement, counterintelligence, and telecom security. That is why, during the first two years of this Administration, we co-led more CFIUS reviews than in the five years before that, combined. That is why we have renamed the staff that conducts these reviews to be a "Section," and reorganized its management structure, to match other operational components of NSD. And that is why the President's proposed budget for the Department would significantly increase the staff and other resources devoted to this work.

II. FIRRMA

In doing so, we are positioning ourselves to be ready to do our part in implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). We are already working closely with the Department of the Treasury to implement the newly launched pilot program under the statute and to develop regulations to implement the Committee's expanded authority.

As this room already knows, FIRRMA represents the most significant reform of the CFIUS process in more than a decade. The Department was pleased to support the act, which adapts CFIUS to address current threats. Most significantly, in my view, it expands the Committee's authority to address emerging national security risks that fall outside foreign control thresholds, such as minority investments that give access to sensitive information or technology, or any deal structured to circumvent CFIUS review.

But FIRRMA is not just about expanding the government's power. I believe the legislation reflects a commitment to increased transparency, predictability, and efficiency in the CFIUS process, a commitment we share. More specifically:

1. The new declaration process mandates that companies contemplating qualifying transactions file

1. The new declaration process mandates that companies contemplating qualifying transactions file short notifications before consummating a transaction, but this "light filing" requires much less information than a voluntary notification, and it allows the Committee to clear low risk transactions much faster (providing certainty to the parties where appropriate) and to identify significant national security issues in other cases before closing.
2. FIRRMA extends the initial review period by 15 days, but even that small increase should allow the Committee to clear more transactions in review and to reduce the need to re-file cases.
3. By specifying that any judicial review occur before the Court of Appeals for the D.C. Circuit, the legislation shortens the time required for judicial review and ensures that a consistent body of precedent develops in one court with extensive experience reviewing administrative decisions.
4. And by giving CFIUS agencies specialized authority to hire additional staff, it ensures that we can manage the additional CFIUS filings that we expect.

In these ways, FIRRMA reflects our longstanding open investment policy, makes the United States an attractive location for foreign investors, and applies neutrally to investment from any country.

By contrast, and as USTR has highlighted in its Section 301 reports, U.S. companies trying to enter the Chinese market must navigate foreign ownership restrictions, joint venture requirements, discriminatory licensing regimes, and vague and discretionary administrative approval processes that allow the Chinese government to pressure them to transfer their technology as a condition of market access.

In seeking to protect against national security risk, we must remember that free enterprise, market incentives, and the exchange of capital, people, and ideas across borders have been critical ingredients to our economic success. The ultimate goal of our foreign investment reviews is to preserve the framework of private choices and freedom that has made our companies and innovations the envy of the world.

Along those lines, we must also work to reform the *ad hoc* process by which the Executive Branch advises the FCC on license applications, known as Team Telecom. Although I am pleased with the ultimate recommendation in the China Mobile matter, which sets an important precedent, we must explore ways to make this process more efficient and expedient, so that the Executive Branch never again takes nearly seven years to make a recommendation.

Conclusion

Despite the threats and challenges we face, last year was a tremendous one for American innovation. In 2018, U.S. companies obtained 142,000 new U.S. utility grant patents out of the more than 308,000 patents that the U.S. Patent and Trademark Office approved. Six of the top 10 U.S. patent recipients were U.S. corporations. As of 2016, industries that rely heavily on intellectual property supported at least 45 million U.S. jobs and contributed more than $6 trillion dollars to, or 38.2 percent of, U.S. gross domestic product.

Last year's headlines offers examples of inventions and advances that are truly miraculous:

- In January, a Massachusetts company introduced the first commercial version of its four-legged, dog-like robot at the Consumer Electronics Show in Las Vegas. This robot can already run, jump, dance, and open doors. The commercial version is being tested for use in construction, work place inspection, and physical security, to name just a few potential uses.
- In April, a California company announced its next generation drone, capable of flying at a speed of up to 80 mph for a range of up to 99 miles round trip while carrying up to 3.9 lbs. Among other uses, drones like this can carry shipments of donated blood or other specialized medical supplies across difficult terrain with few paved roads.
- In June, a Massachusetts medical device company conducted a groundbreaking two week study of their Closed-Loop insulin delivery system. The system is essentially a bionic pancreas, one of a handful of FDA-approved technologies that combines both a glucose monitor and insulin pump to almost entirely automate blood sugar control in type 1 diabetics. The study showed that in normal living conditions Type 1 diabetics could better control blood sugar and reduce incidences of hypoglycemia with the closed loop system; no finger pricks required.
- A U.S. automaker released a luxury sedan with its new semiautonomous, hands-free driver assistance technology. This technology relies upon LiDAR (or laser sensors that work like radar)

assistance technology. This technology relies upon LIDAR (or laser sensors that work like radar) mapping, in-car cameras, radar sensors, and GPS to detect the road ahead, control speed, and maintain lane position while allowing the driver to travel without touching the wheel or pedals. You still need to pay attention to the road, however, and if the driver begins to nod off or get distracted, the vehicle will alert the driver through a series of escalating vibrations and chimes. This automaker has announced plans to install the semiautonomous technology in all new vehicles by 2020, moving us one-step closer to safe, self-driving vehicles on U.S. road.

- Finally, in December 2018, a California company conducted a test flight of a manned, suborbital plane designed for space tourism. The flight, which was the fastest and highest commercial test flight to-date, reached a peak altitude of roughly 51 miles above the Earth's surface. It was the first time a commercial vehicle designed for tourism entered outer space.

I believe that, if we get it right---if we balance tailored authorities and a focus on national security with respect for free markets---we will continue to see unparalleled innovations like these in the United States, fueled in no small part by foreign investment. And in the coming year, I look forward to working with you to strike that balance.

# # #

NSD

19-416

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: Hamilton, Gene (OAG)
Subject: FW: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES
To: Risch, Carl C
Sent: January 28, 2020 12:48 PM (UTC-05:00)

Gene P. Hamilton
Counselor to the Attorney General
U.S. Department of Justice

From: USDOJ-Office of Public Affairs <(b) (6)
Sent: Tuesday, January 28, 2020 12:23 PM
To: Hamilton, Gene (OAG) <(b) (6)
Subject: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JANUARY 28, 2020
WWW.JUSTICE.GOV/NEWS

NOTE: The charging documents can be found here.

HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

WASHINGTON – The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B.

Bowler in federal court in Boston.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the

Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey,

Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

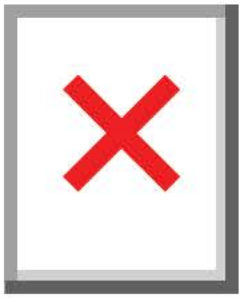
# # #

NSD

20-99

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES
To: Schreiber, Jayne (OAG)
Sent: January 28, 2020 12:23 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, JANUARY 28, 2020

NOTE: The charging documents can be found here.

HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

WASHINGTON – The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a

materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B. Bowler in federal court in Boston.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During

the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey, Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

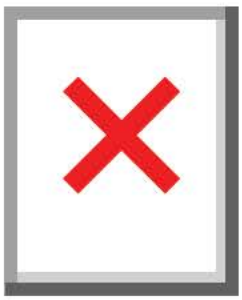
# # #

NSD

20-99

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES
To: Bissex, Rachel (OAG)
Sent: January 28, 2020 12:23 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, JANUARY 28, 2020

NOTE: The charging documents can be found here.

HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

WASHINGTON – The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a

materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B. Bowler in federal court in Boston.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During

the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey, Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

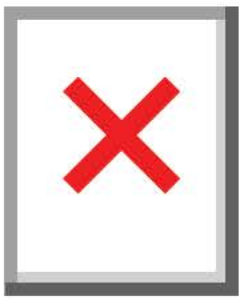
# # #

NSD

20-99

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES
To: Hamilton, Gene (OAG)
Sent: January 28, 2020 12:23 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, JANUARY 28, 2020

NOTE: The charging documents can be found here.

HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

WASHINGTON – The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a

materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B. Bowler in federal court in Boston.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During

the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey, Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

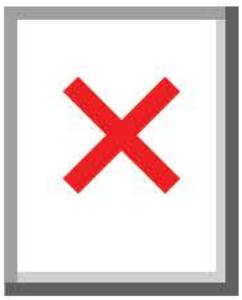
# # #

NSD

20-99

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES
To: Watson, Theresa (OAG)
Sent: January 28, 2020 12:23 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, JANUARY 28, 2020

NOTE: The charging documents can be found here.

HARVARD UNIVERSITY PROFESSOR AND TWO CHINESE NATIONALS CHARGED IN THREE SEPARATE CHINA RELATED CASES

WASHINGTON – The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a

materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B. Bowler in federal court in Boston.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During

the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey, Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

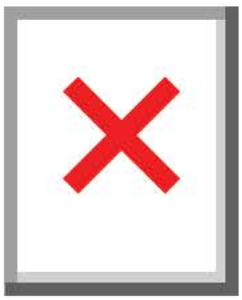
# # #

NSD

20-99

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS
To: Schreiber, Jayne (OAG)
Sent: November 12, 2019 4:13 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE **TUESDAY, NOVEMBER 12, 2019**
WWW.JUSTICE.GOV/NEWS

CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS

WASHINGTON – Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, pleaded guilty Tuesday in federal court to committing theft of trade secrets from his employer, a U.S. petroleum company.

Tan pleaded guilty to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. The defendant stole the information from a U.S.-based petroleum company regarding the manufacture of a "research and development downstream energy market product" that is worth more than $1 billion.

"Tan's guilty plea continues to fill in the picture of China's theft of American intellectual property," said Assistant Attorney General for National Security John C. Demers. "The Department launched its China Initiative to battle precisely the type of behavior reflected in today's plea — illegal behavior that costs Americans their jobs — and we will continue to do so."

"China's economic aggression poses a threat to America's emerging high-technology industries. Industrial spies like Hongjin Tan engage in espionage to steal American trade secrets and intellectual property born out of the innovation that is innate in our free market system," said U.S. Attorney Trent Shores for the Northern District of Oklahoma. "Thanks to a vigilant company and the investigative efforts of the FBI, Hongjin Tan was caught red handed and prosecuted. American ingenuity and know-how are the envy of the international market, and the U.S. Attorneys community will work to protect our economic infrastructure."

"Trade secret theft is a serious crime which hurts American businesses and taxpayers. The FBI will continue to protect our country's industries from adversaries who attempt to steal valuable research and technology," said FBI Special Agent in Charge Melissa Godbold of the Oklahoma City Field Office.

Tan was employed as an associate scientist for the U.S. petroleum company starting in June 2017 until his arrest in December 2018. The defendant was assigned to work within a group at the company with the goal of developing next generation battery technologies for stationary energy storage, specifically flow batteries. In his plea agreement, Tan admitted to intentionally copying and downloading research and development materials without authorization from his employer.

On Dec. 11, 2018, Tan used a thumb drive to copy hundreds of files. He subsequently turned in his resignation and was escorted from the premises on Dec. 12, 2018. Later that day, he returned the thumb drive, claiming that he had forgotten to do so before leaving his employer's property. Upon examination, it was discovered that there was unallocated space on the thumb drive, indicating five documents had previously been deleted. Investigators with the FBI searched Tan's premises and found an external hard drive. They discovered that the same five missing files from the thumb drive had been downloaded to the hard drive. Tan maintained the files on a hard drive so he could access the data at a later date. Further accessing the material would have been financially advantageous for Tan but caused significant financial damage to his Oklahoma employer.

U.S. District Judge Gregory K. Frizzell presided over the plea hearing and set sentencing for Feb. 12, 2020.

The FBI conducted this investigation. Assistant U.S. Attorney Joel-lyn A. McCormick of the Northern District of Oklahoma and Trial Attorney Matthew J. McKenzie of the National Security Division's Counterintelligence and Export Control Section (CES) are prosecuting the case, with assistance from Trial Attorney Matthew R. Walczewski and Assistant Deputy Chief Brian J. Resler of the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS).

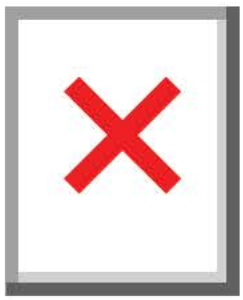
# # #

NSD

19-1232

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS
To: Bissex, Rachel (OAG)
Sent: November 12, 2019 4:13 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, NOVEMBER 12, 2019

CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS

WASHINGTON – Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, pleaded guilty Tuesday in federal court to committing theft of trade secrets from his employer, a U.S. petroleum company.

Tan pleaded guilty to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. The defendant stole the information from a U.S.-based petroleum company regarding the manufacture of a "research and development downstream energy market product" that is worth more than $1 billion.

"Tan's guilty plea continues to fill in the picture of China's theft of American intellectual property," said Assistant Attorney General for National Security John C. Demers. "The Department launched its China Initiative to battle precisely the type of behavior reflected in today's plea — illegal behavior that costs Americans their jobs — and we will continue to do so."

"China's economic aggression poses a threat to America's emerging high-technology industries. Industrial spies like Hongjin Tan engage in espionage to steal American trade secrets and intellectual property born out of the innovation that is innate in our free market system," said U.S. Attorney Trent Shores for the Northern District of Oklahoma. "Thanks to a vigilant company and the investigative efforts of the FBI, Hongjin Tan was caught red handed and prosecuted. American ingenuity and know-how are the envy of the international market, and the U.S. Attorneys community will work to protect our economic infrastructure."

"Trade secret theft is a serious crime which hurts American businesses and taxpayers. The FBI will continue to protect our country's industries from adversaries who attempt to steal valuable research and technology," said FBI Special Agent in Charge Melissa Godbold of the Oklahoma City Field Office.

Tan was employed as an associate scientist for the U.S. petroleum company starting in June 2017 until his arrest in December 2018. The defendant was assigned to work within a group at the company with the goal of developing next generation battery technologies for stationary energy storage, specifically flow batteries. In his plea agreement, Tan admitted to intentionally copying and downloading research and development materials without authorization from his employer.

On Dec. 11, 2018, Tan used a thumb drive to copy hundreds of files. He subsequently turned in his resignation and was escorted from the premises on Dec. 12, 2018. Later that day, he returned the thumb drive, claiming that he had forgotten to do so before leaving his employer's property. Upon examination, it was discovered that there was unallocated space on the thumb drive, indicating five documents had previously been deleted. Investigators with the FBI searched Tan's premises and found an external hard drive. They discovered that the same five missing files from the thumb drive had been downloaded to the hard drive. Tan maintained the files on a hard drive so he could access the data at a later date. Further accessing the material would have been financially advantageous for Tan but caused significant financial damage to his Oklahoma employer.

U.S. District Judge Gregory K. Frizzell presided over the plea hearing and set sentencing for Feb. 12, 2020.

The FBI conducted this investigation. Assistant U.S. Attorney Joel-lyn A. McCormick of the Northern District of Oklahoma and Trial Attorney Matthew J. McKenzie of the National Security Division's Counterintelligence and Export Control Section (CES) are prosecuting the case, with assistance from Trial Attorney Matthew R. Walczewski and Assistant Deputy Chief Brian J. Resler of the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS).

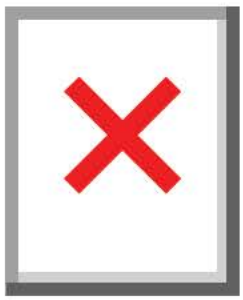
# # #

NSD

19-1232

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS
To: Hamilton, Gene (OAG)
Sent: November 12, 2019 4:13 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

TUESDAY, NOVEMBER 12, 2019

CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS

WASHINGTON – Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, pleaded guilty Tuesday in federal court to committing theft of trade secrets from his employer, a U.S. petroleum company.

Tan pleaded guilty to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. The defendant stole the information from a U.S.-based petroleum company regarding the manufacture of a "research and development downstream energy market product" that is worth more than $1 billion.

"Tan's guilty plea continues to fill in the picture of China's theft of American intellectual property," said Assistant Attorney General for National Security John C. Demers. "The Department launched its China Initiative to battle precisely the type of behavior reflected in today's plea — illegal behavior that costs Americans their jobs — and we will continue to do so."

"China's economic aggression poses a threat to America's emerging high-technology industries. Industrial spies like Hongjin Tan engage in espionage to steal American trade secrets and intellectual property born out of the innovation that is innate in our free market system," said U.S. Attorney Trent Shores for the Northern District of Oklahoma. "Thanks to a vigilant company and the investigative efforts of the FBI, Hongjin Tan was caught red handed and prosecuted. American ingenuity and know-how are the envy of the international market, and the U.S. Attorneys community will work to protect our economic infrastructure."

"Trade secret theft is a serious crime which hurts American businesses and taxpayers. The FBI will continue to protect our country's industries from adversaries who attempt to steal valuable research and technology," said FBI Special Agent in Charge Melissa Godbold of the Oklahoma City Field Office.

Tan was employed as an associate scientist for the U.S. petroleum company starting in June 2017 until his arrest in December 2018. The defendant was assigned to work within a group at the company with the goal of developing next generation battery technologies for stationary energy storage, specifically flow batteries. In his plea agreement, Tan admitted to intentionally copying and downloading research and development materials without authorization from his employer.

On Dec. 11, 2018, Tan used a thumb drive to copy hundreds of files. He subsequently turned in his resignation and was escorted from the premises on Dec. 12, 2018. Later that day, he returned the thumb drive, claiming that he had forgotten to do so before leaving his employer's property. Upon examination, it was discovered that there was unallocated space on the thumb drive, indicating five documents had previously been deleted. Investigators with the FBI searched Tan's premises and found an external hard drive. They discovered that the same five missing files from the thumb drive had been downloaded to the hard drive. Tan maintained the files on a hard drive so he could access the data at a later date. Further accessing the material would have been financially advantageous for Tan but caused significant financial damage to his Oklahoma employer.

U.S. District Judge Gregory K. Frizzell presided over the plea hearing and set sentencing for Feb. 12, 2020.

The FBI conducted this investigation. Assistant U.S. Attorney Joel-lyn A. McCormick of the Northern District of Oklahoma and Trial Attorney Matthew J. McKenzie of the National Security Division's Counterintelligence and Export Control Section (CES) are prosecuting the case, with assistance from Trial Attorney Matthew R. Walczewski and Assistant Deputy Chief Brian J. Resler of the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS).

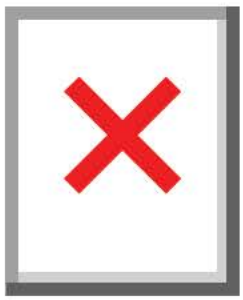
# # #

NSD

19-1232

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS
To: Watson, Theresa (OAG)
Sent: November 12, 2019 4:13 PM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE **TUESDAY, NOVEMBER 12, 2019**
WWW.JUSTICE.GOV/NEWS

CHINESE NATIONAL PLEADS GUILTY TO COMMITTING THEFT OF TRADE SECRETS

WASHINGTON – Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, pleaded guilty Tuesday in federal court to committing theft of trade secrets from his employer, a U.S. petroleum company.

Tan pleaded guilty to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. The defendant stole the information from a U.S.-based petroleum company regarding the manufacture of a "research and development downstream energy market product" that is worth more than $1 billion.

"Tan's guilty plea continues to fill in the picture of China's theft of American intellectual property," said Assistant Attorney General for National Security John C. Demers. "The Department launched its China Initiative to battle precisely the type of behavior reflected in today's plea — illegal behavior that costs Americans their jobs — and we will continue to do so."

"China's economic aggression poses a threat to America's emerging high-technology industries. Industrial spies like Hongjin Tan engage in espionage to steal American trade secrets and intellectual property born out of the innovation that is innate in our free market system," said U.S. Attorney Trent Shores for the Northern District of Oklahoma. "Thanks to a vigilant company and the investigative efforts of the FBI, Hongjin Tan was caught red handed and prosecuted. American ingenuity and know-how are the envy of the international market, and the U.S. Attorneys community will work to protect our economic infrastructure."

"Trade secret theft is a serious crime which hurts American businesses and taxpayers. The FBI will continue to protect our country's industries from adversaries who attempt to steal valuable research and technology," said FBI Special Agent in Charge Melissa Godbold of the Oklahoma City Field Office.

Tan was employed as an associate scientist for the U.S. petroleum company starting in June 2017 until his arrest in December 2018. The defendant was assigned to work within a group at the company with the goal of developing next generation battery technologies for stationary energy storage, specifically flow batteries. In his plea agreement, Tan admitted to intentionally copying and downloading research and development materials without authorization from his employer.

On Dec. 11, 2018, Tan used a thumb drive to copy hundreds of files. He subsequently turned in his resignation and was escorted from the premises on Dec. 12, 2018. Later that day, he returned the thumb drive, claiming that he had forgotten to do so before leaving his employer's property. Upon examination, it was discovered that there was unallocated space on the thumb drive, indicating five documents had previously been deleted. Investigators with the FBI searched Tan's premises and found an external hard drive. They discovered that the same five missing files from the thumb drive had been downloaded to the hard drive. Tan maintained the files on a hard drive so he could access the data at a later date. Further accessing the material would have been financially advantageous for Tan but caused significant financial damage to his Oklahoma employer.

U.S. District Judge Gregory K. Frizzell presided over the plea hearing and set sentencing for Feb. 12, 2020.

The FBI conducted this investigation. Assistant U.S. Attorney Joel-lyn A. McCormick of the Northern District of Oklahoma and Trial Attorney Matthew J. McKenzie of the National Security Division's Counterintelligence and Export Control Section (CES) are prosecuting the case, with assistance from Trial Attorney Matthew R. Walczewski and Assistant Deputy Chief Brian J. Resler of the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS).

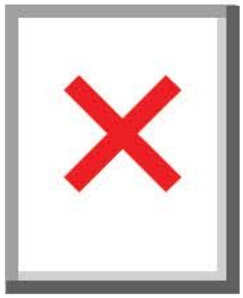
# # #

NSD

19-1232

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS
To: Bryant, Errical (OAG)
Sent: July 2, 2019 2:44 PM (UTC-04:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 2, 2019

Note: You can find more information about the Department's China Initiative here.

ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS

WASHINGTON – An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the

announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

“The Department’s China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China,” said Assistant Attorney General Demers. “The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution.”

“This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns,” said U.S. Attorney Nick Hanna. “My office will enforce laws that protect our nation’s intellectual property from being used to benefit foreign adversaries who may compromise our national security.”

“The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research,” said Assistant Director in Charge Delacourt. “We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security.”

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company’s computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih’s true intent to transfer the U.S. company’s products to the People’s Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company’s semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents, “due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.”

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company.

Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

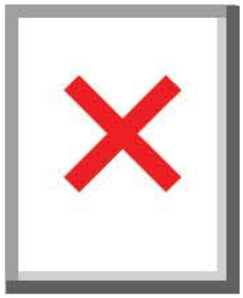
# # #

NSD

19-735

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS
To: Bissex, Rachel (OAG)
Sent: July 2, 2019 2:44 PM (UTC-04:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 2, 2019

Note: You can find more information about the Department's China Initiative here.

ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS

WASHINGTON – An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the

announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

“The Department’s China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China,” said Assistant Attorney General Demers. “The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution.”

“This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns,” said U.S. Attorney Nick Hanna. “My office will enforce laws that protect our nation’s intellectual property from being used to benefit foreign adversaries who may compromise our national security.”

“The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research,” said Assistant Director in Charge Delacourt. “We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security.”

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company’s computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih’s true intent to transfer the U.S. company’s products to the People’s Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company’s semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents, “due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.”

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company.

Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

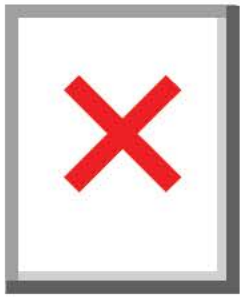
# # #

NSD

19-735

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS
To: Hamilton, Gene (OAG)
Sent: July 2, 2019 2:44 PM (UTC-04:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 2, 2019

Note: You can find more information about the Department's China Initiative here.

ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS

WASHINGTON – An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the

announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

“The Department’s China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China,” said Assistant Attorney General Demers. “The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution.”

“This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns,” said U.S. Attorney Nick Hanna. “My office will enforce laws that protect our nation’s intellectual property from being used to benefit foreign adversaries who may compromise our national security.”

“The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research,” said Assistant Director in Charge Delacourt. “We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security.”

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company’s computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih’s true intent to transfer the U.S. company’s products to the People’s Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company’s semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents, “due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.”

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company.

Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

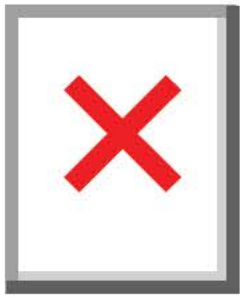
# # #

NSD

19-735

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS
To: Morrissey, Brian (OAG)
Sent: July 2, 2019 2:44 PM (UTC-04:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 2, 2019

Note: You can find more information about the Department's China Initiative here.

ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS

WASHINGTON – An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the

announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

“The Department’s China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China,” said Assistant Attorney General Demers. “The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution.”

“This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns,” said U.S. Attorney Nick Hanna. “My office will enforce laws that protect our nation’s intellectual property from being used to benefit foreign adversaries who may compromise our national security.”

“The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research,” said Assistant Director in Charge Delacourt. “We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security.”

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company’s computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih’s true intent to transfer the U.S. company’s products to the People’s Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company’s semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents, “due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.”

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company.

Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

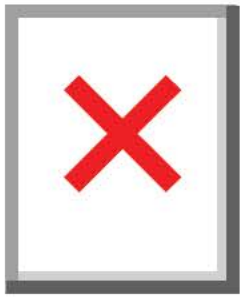
# # #

NSD

19-735

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS
To: Watson, Theresa (OAG)
Sent: July 2, 2019 2:44 PM (UTC-04:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 2, 2019

Note: You can find more information about the Department's China Initiative here.

ELECTRICAL ENGINEER CONVICTED OF CONSPIRING TO ILLEGALLY EXPORT TO CHINA SEMICONDUCTOR CHIPS WITH MISSILE GUIDANCE APPLICATIONS

WASHINGTON – An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the

announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

“The Department’s China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China,” said Assistant Attorney General Demers. “The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution.”

“This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns,” said U.S. Attorney Nick Hanna. “My office will enforce laws that protect our nation’s intellectual property from being used to benefit foreign adversaries who may compromise our national security.”

“The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research,” said Assistant Director in Charge Delacourt. “We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security.”

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company’s computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih’s true intent to transfer the U.S. company’s products to the People’s Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company’s semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents, “due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.”

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company.

Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

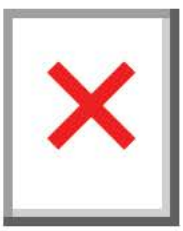
# # #

NSD

19-735

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Barnett, Gary E. (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

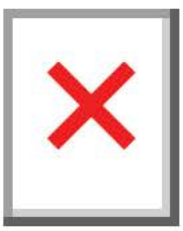
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Watson, Theresa (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

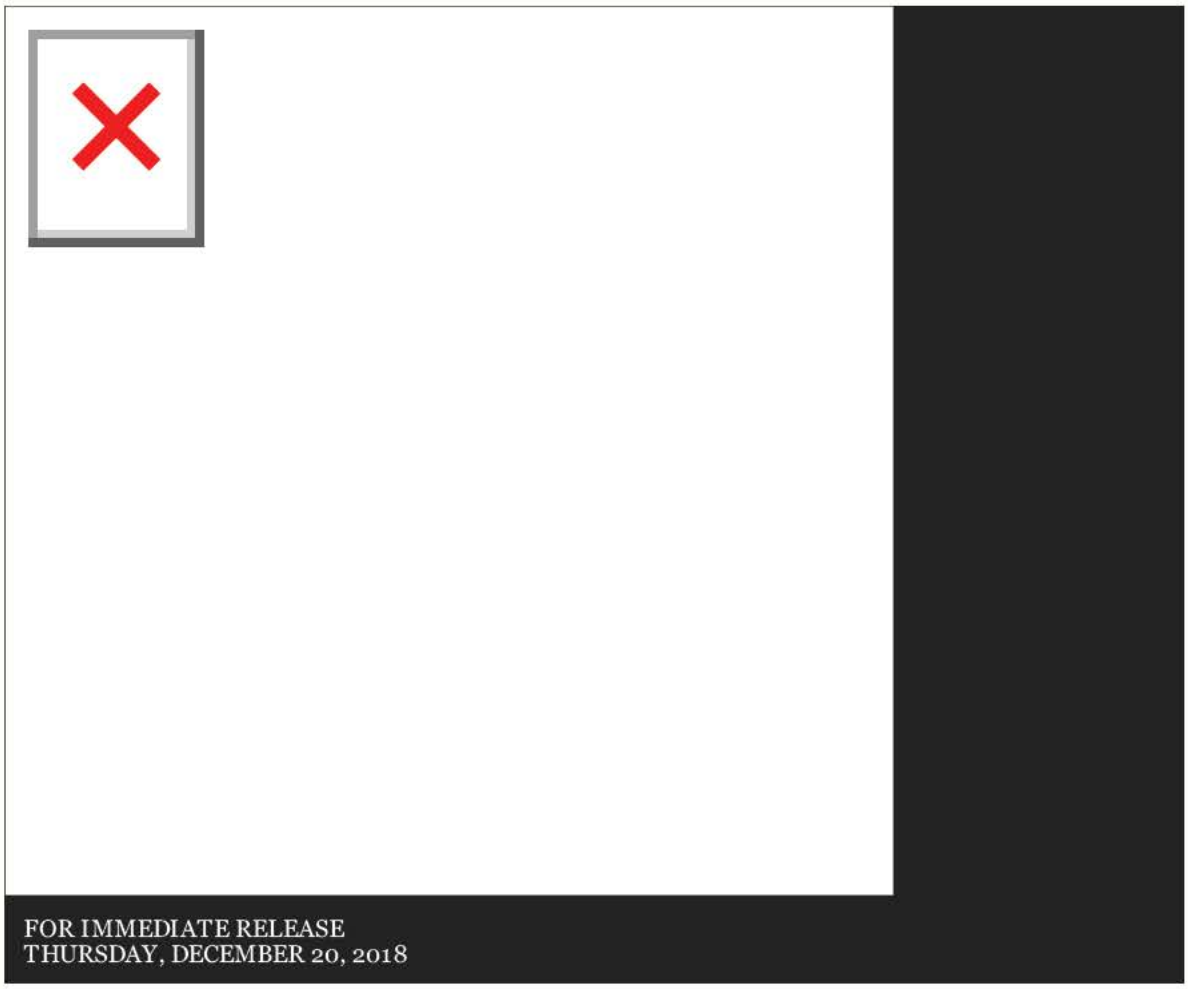
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Tucker, Rachael (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

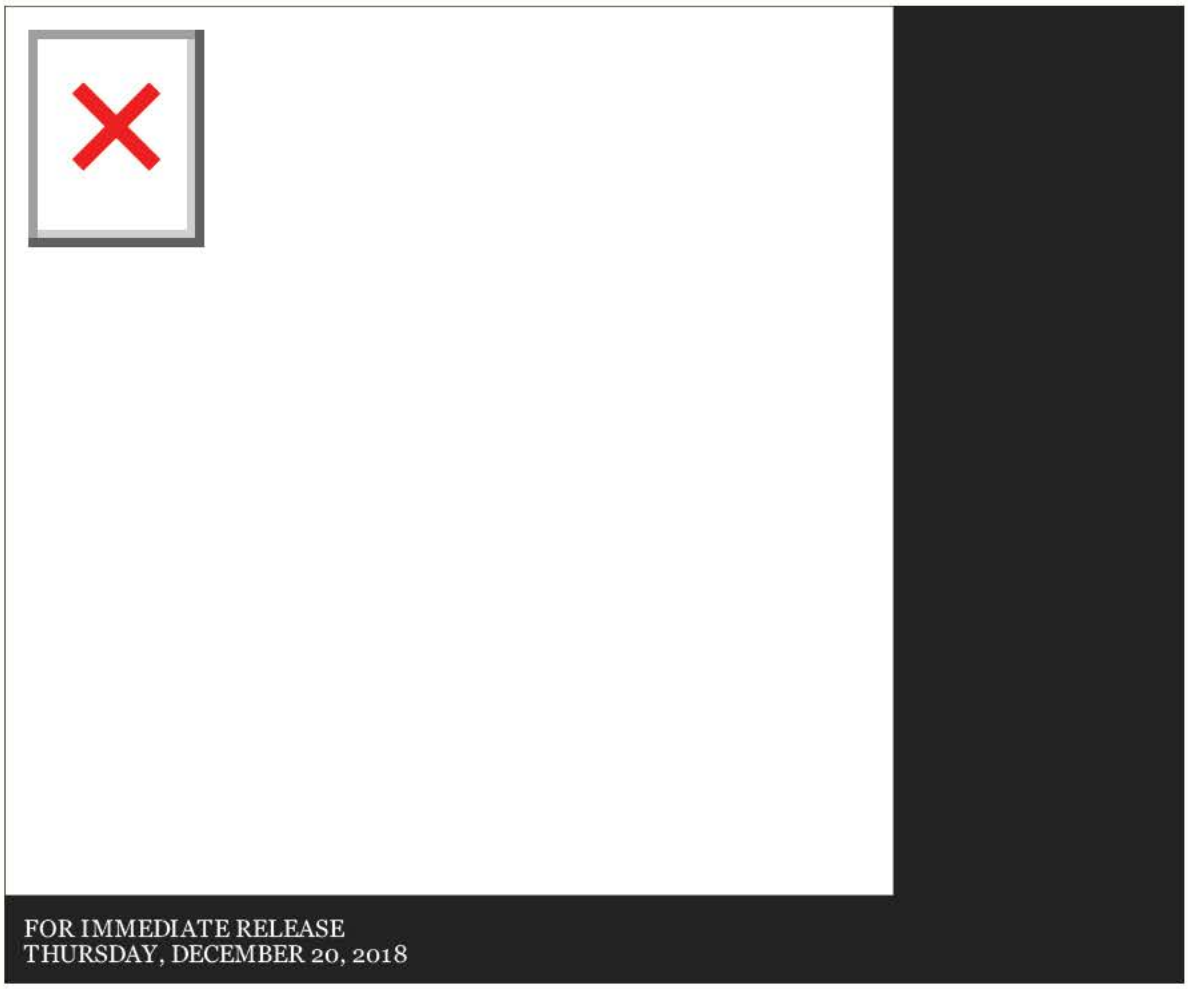
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Bumatay, Patrick (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

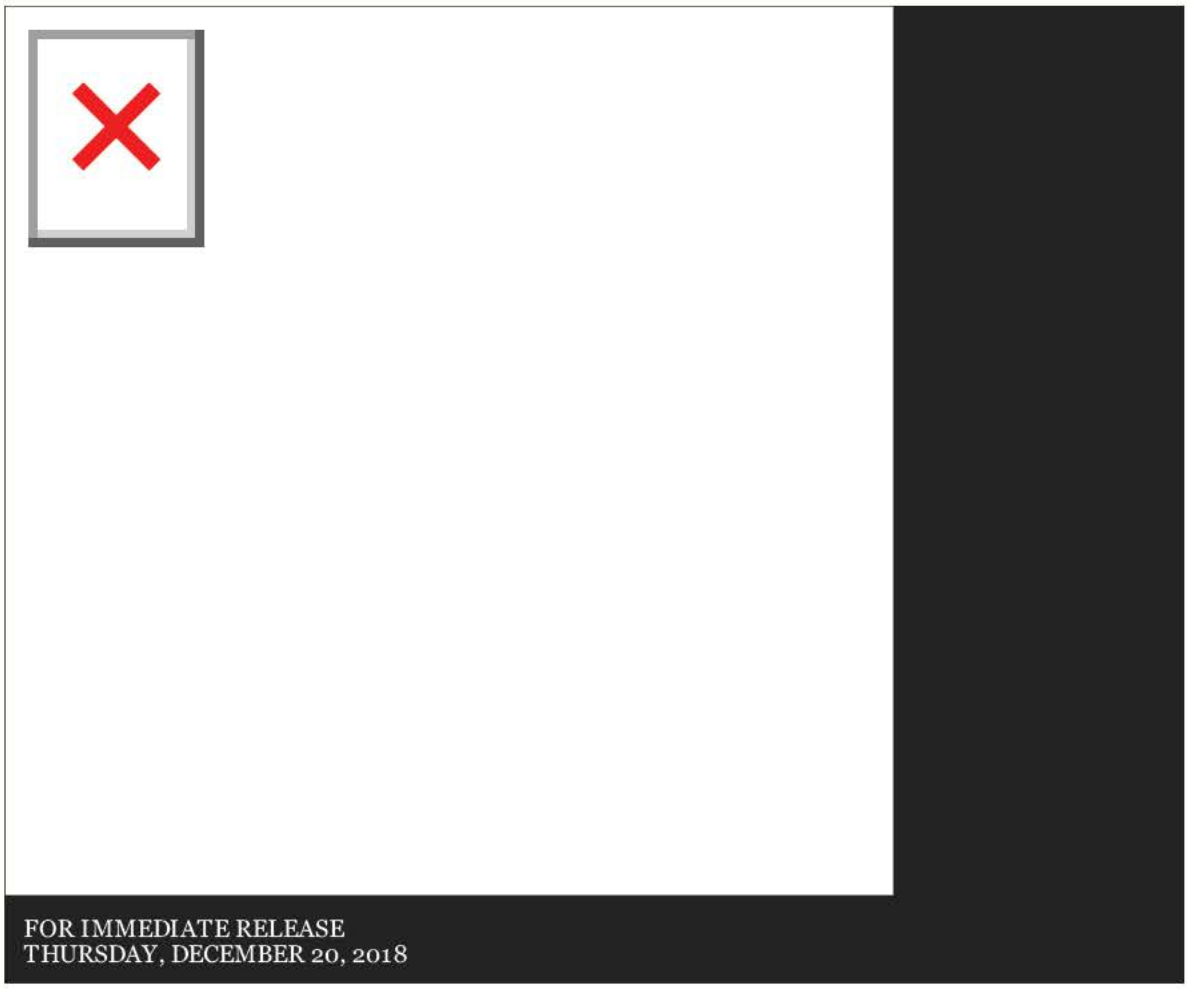
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Allen, Alexis (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

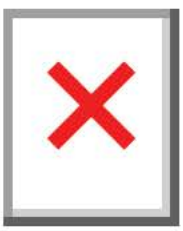
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Bryant, Errical (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

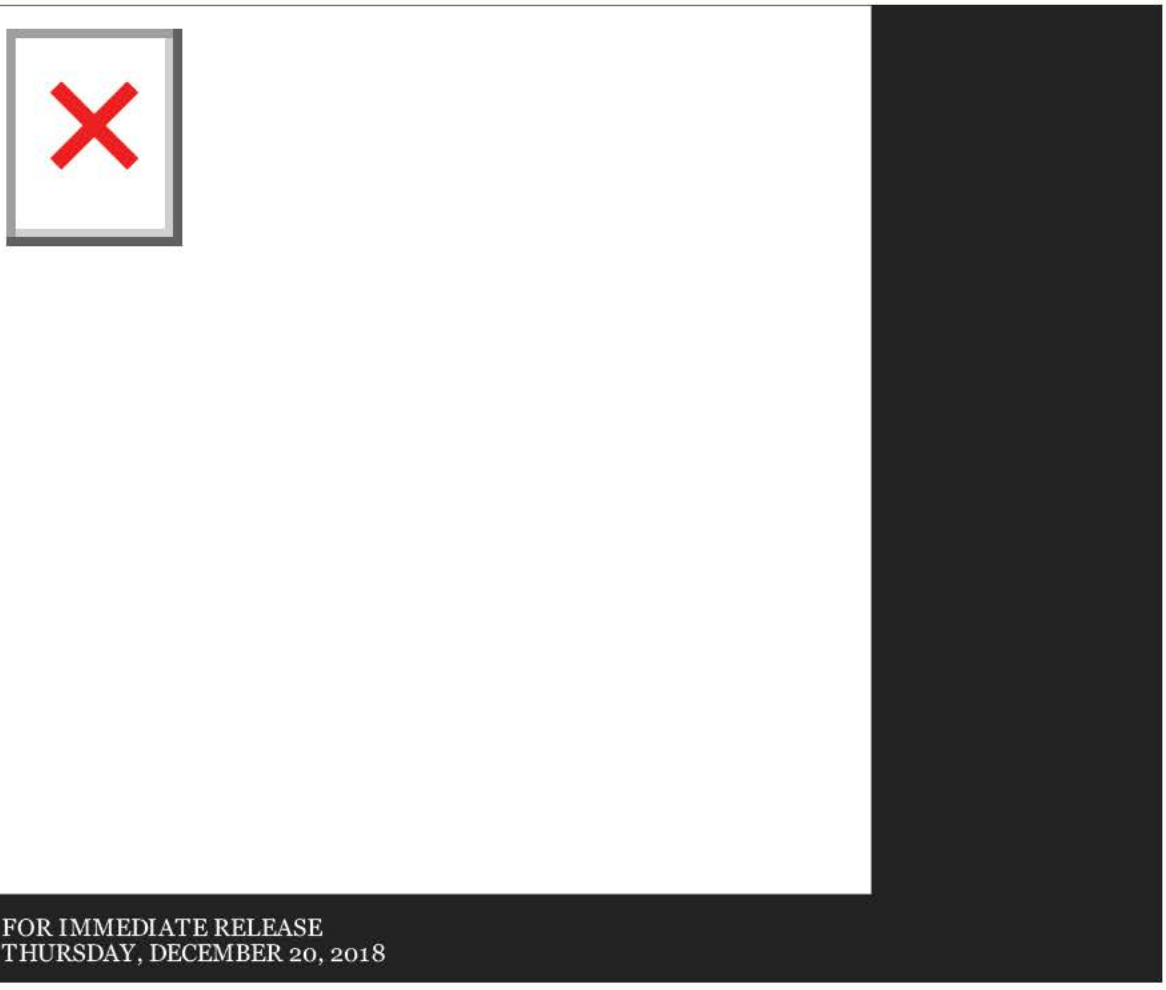
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Hamilton, Gene (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

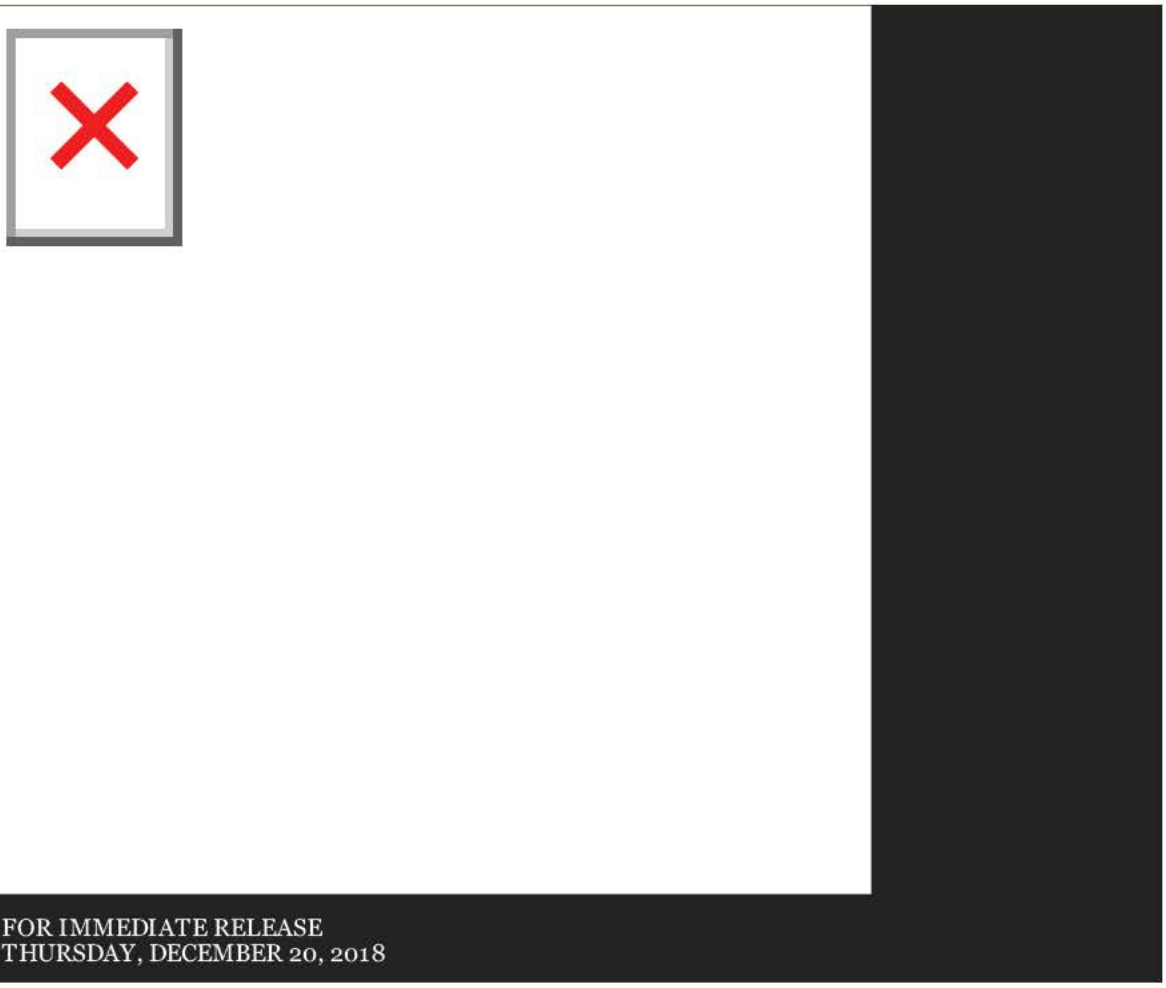
# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: USDOJ-Office of Public Affairs
Subject: TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION
To: Morrissey, Brian (OAG)
Sent: December 20, 2018 10:42 AM (UTC-05:00)



FOR IMMEDIATE RELEASE
THURSDAY, DECEMBER 20, 2018

NOTE: The *Department of Justice China Initiative Fact Sheet* can be found here, and the *Year in Review for China Related Cases* can be found here.

TWO CHINESE HACKERS ASSOCIATED WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGNS TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

WASHINGTON – The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The

APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology;

three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.

# # #

NSD

18-1673

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

From: Coley, Anthony D. (PAO)
Subject: Abbreviated AM Clips
To: Klapper, Matthew B. (OAG)
Cc: Iverson, Dena (PAO); Heinzelman, Kate (OAG); Goodlander, Margaret V. (OAG); Matthews-Johnson, Tamarra D. (OAG); Visser, Tim (OAG); Reich, Mitchell (OAG)
Sent: December 15, 2021 7:12 AM (UTC-05:00)

MORNING HEADLINES

- "House votes to hold Meadows in contempt over Jan. 6 panel subpoena" [WaPo, NYT, LAT, WSJ]

NATIONAL SECURITY

AP: **Harvard Professor's Trial a Test of DOJ's China Prosecutions,** Philip Marcelo, December 14, 2021, 3:42 PM
The trial of a Harvard University professor charged with hiding his ties to a Chinese-run recruitment program is the latest bellwether in the U.S. Justice Department's controversial effort to crackdown on economic espionage by China. Opening statements in the trial of Charles Lieber, the former chair of Harvard's department of chemistry and chemical biology, begin Wednesday after jury selection was completed Tuesday in Boston federal court. [Continue Reading] **See also:** Washington Examiner, WSJ

CNN: **US government to offer up to $5,000 'bounty' to hackers to identify cyber vulnerabilities,** Geneva Sands, December 14, 2021, 8:09 PM
The Department of Homeland Security is launching a "bug bounty" program, potentially offering thousands of dollars to hackers who help the department identify cybersecurity vulnerabilities within its systems. DHS will pay between $500 and $5,000 depending on the gravity of the vulnerability and the impact of the remediation, Homeland Security Secretary Alejandro Mayorkas announced Tuesday. [Continue Reading]

CNN: **US warns hundreds of millions of devices at risk from newly revealed software vulnerability,** Sean Lyngaas, December 14, 2021, 3:55 PM
Hundreds of millions of devices around the world could be exposed to a newly revealed software vulnerability, as a senior Biden administration cyber official warned executives from major US industries Monday that they need to take action to address "one of the most serious" flaws she has seen in her career. As major tech firms struggle to contain the fallout, US officials held a call with industry executives warning that hackers are actively exploiting the vulnerability. [Continue Reading] **See also:** The Hill

Forbes: **Iranian Hackers Abuse Slack For Cyber Spying,** Thomas Brewster, December 15, 2021, 6:00 AM
IBM researchers claim an Iranian-linked crew called MuddyWater has been trying to avoid detection by using Slack to control their malware. It's believed to be the first time a suspected state-backed hacking outfit has been seen using such a technique. Back in March, hackers believed to be Iranian cyber spies found a novel use for the workplace messaging app Slack. They'd broken into an Asian airline and installed a backdoor. [Continue Reading]

JAN. 6

AP: **House votes to hold Mark Meadows in contempt in Jan. 6 probe**, Farnoush Amiri and Mary Clare Jalonick, December 14, 2021, 11:00 PM
The House voted Tuesday to hold former White House chief of staff Mark Meadows in contempt of Congress after he ceased to cooperate with the Jan. 6 Committee investigating the Capitol insurrection — making it the first time the House has voted to hold a former member in contempt since the 1830s. The near-party-line 222-208 vote is the second time the special committee has sought to punish a witness for defying a subpoena. [Continue Reading] **See also:** Business Insider, Courthouse New, CBS,

CNN, Guardian, The Hill, HuffPost, LAT, NBC, NPR, NYT, Reuters, USA Today, WaPo, Washington Examiner, WSJ

WaPo: **Text messages to Meadows renew focus on Trump's inaction during Jan. 6 attack,** Amy B Wang, December 14, 2021, 7:21 PM
Newly released text messages that were sent on Jan. 6 to Mark Meadows, a former chief of staff in the Trump White House, have put a renewed focus on President Donald Trump's failure to act quickly to stop the insurrection at the U.S. Capitol as it was unfolding, despite real-time pleas from lawmakers, journalists and even his eldest son. At least half a dozen people reached out during the riot to Meadows to ask — in some cases, beg — Trump to intervene, according to text messages detailed this week by Rep. Liz Cheney (R-Wyo.), the vice chair of the House select committee investigating the attack. [Continue Reading]

Insider: **Meet Steve Bannon's prosecutor, the most important Justice Department official you've never heard of,** C. Ryan Barber, December 14, 2021, 1:30 PM
The federal prosecutors knew that, if they didn't bring charges, Republicans would accuse the sitting Democratic administration of protecting one of its own. So the decision could not have a whiff of politics. It was late in the Obama presidency, and House Republicans had referred a top IRS official to the Justice Department in a scandal over whether the tax agency had improperly targeted conservative groups. [Continue Reading]

WaPo: **D.C. attorney general sues Proud Boys, Oath Keepers over Jan. 6 attack,** Devlin Barrett, Tom Hamburger, and Rachel Weiner, December 14, 2021, 11:45 AM
D.C. Attorney General Karl A. Racine (D) on Tuesday sued the Proud Boys and Oath Keepers over the Jan. 6 attack on Congress, seeking to use a law written to cripple the Ku Klux Klan to exact stiff financial penalties from the far-right groups that Racine alleges were responsible for the violence. The lawsuit filed in federal court in Washington, D.C., cites the modern version of an 1871 law known as the Ku Klux Klan Act, which was enacted after the Civil War to safeguard government officials carrying out their duties and protect civil rights. [Continue Reading] **See also:** BuzzFeed, CNN, Guardian, The Hill, NPR, NPR-2, Washington Times, WSJ

WaPo: **Congress votes to let Capitol Police chief directly call on National Guard, law enforcement after Jan. 6 riot,** Bryan Pietsch, December 15, 2021, 5:07 AM
Congress on Tuesday passed legislation granting the Capitol Police chief power to "unilaterally" request emergency backup from the National Guard and federal law enforcement agencies, after lawmakers said the lack of authority had caused "unnecessary delays" during the Jan. 6 insurrection. The bill passed the Senate and the House of Representatives by unanimous consent and will head to President Biden's desk to be signed into law. [Continue Reading]

WaPo: **[ANALYSIS] No, Trump did not order 10,000 troops to secure the Capitol on Jan. 6,** Glenn Kessler, December 15, 2021, 3:00 AM
"Don't forget, President Trump requested increased National Guard support in the days leading up to January 6. The request was rejected — by Pelosi, by congressional leaders, including requests, by the way, from the Capitol Police chief." — Sean Hannity of Fox News, speaking to former White House chief of staff Mark Meadows, Dec. 13 [Continue Reading]

CRIMINAL LAW

Fox: **Former Louisiana police chief indicted in vote-buying scheme**, Andrew Mark Miller, December 14, 2021, 8:00 PM
A former Louisiana police chief and a current city council member have been indicted on criminal charges over an alleged scheme to buy votes in a federal election. According to a Department of Justice press

release on Tuesday, a federal grand jury indicted former Amite City Police Chief Jerry Trabona and Amite City Council Member Kristian Hart with violating federal election laws. [Continue Reading] **See also:** The Advocate (Baton Rouge, LA), WAFB-CBS (Baton Rouge, LA), WDSU-NBC (New Orleans, LA), WWL-CBS (New Orleans, LA)

CNN: **Man who threatened to shoot Pelosi sentenced to more than two years in prison,** Unattributed, December 14, 2021, 4:04 PM
A Georgia man who drove cross-country with an assault rifle and threatened to kill House Speaker Nancy Pelosi was sentenced to 28 months behind bars in an emotional hearing on Tuesday. Cleveland Meredith Jr. pleaded guilty in September to sending threatening communications. Though he missed the January 6 rally because of car troubles, Meredith was one of the first people charged in relation to the Capitol riot after his mother reported concerning texts to the FBI on January 7. [Continue Reading] **See also:** The Atlanta Journal-Constitution, BuzzFeed, Forbes, The Hill, HuffPost, Politico, UPI, WUSA-CBS (Washington, DC)

Law360: **New DOJ Crime Chief On Boosting Morale And Diversity,** Jack Queen, December 14, 2021, 4:28 PM
Face time with subordinates is a mainstay of U. S. Department of Justice Criminal Division chief Kenneth Polite's management style. After just four months on the job, he's already well-known in the cavernous halls of Main Justice. U. S. Department of Justice Criminal Division chief Kenneth Polite during an interview with Law360. [Continue Reading]

WSJ: **Another Son of Ex-Panama President Pleads Guilty in Odebrecht Bribery Case**, Richard Vanderford, December 14, 2021, 6:16 PM
Another son of former Panamanian President Ricardo Martinelli pleaded guilty to a U.S. charge related to his role in a bribery scheme involving Brazil's Odebrecht SA. Ricardo Alberto Martinelli on Tuesday entered a guilty plea to a single money laundering conspiracy charge at a hearing in federal court in Brooklyn, N.Y. He was charged in 2020 alongside his brother Luis Enrique Martinelli, who pleaded guilty earlier this month. [Continue Reading]

Lakes Tribune (Detroit, MI): **Second Canadian man gets prison after being caught with dozens of guns near Fergus Falls**, Unattributed, December 14, 2021, 4:31 PM
A second Canadian man, caught near Fergus Falls with 67 guns, was sentenced to 68 months in prison for aiding and abetting unlawful possession of firearms, announced Acting United States Attorney Charles J. Kovats. According to court documents, on Jan. 10, 2021, Muzamil Aden Addow, 30, and co-defendant Dayne Adrian Sitladeen, 29, were stopped by a Minnesota State Patrol Trooper near Fergus Falls. The defendants were traveling between 95-100 miles per hour in a Chevrolet Silverado pickup truck with Texas license plates. When the trooper approached the vehicle, Muzamil Aden Addow, the driver, provided an Ontario, Canada, driver's license with a false name. [Continue Reading]

CIVIL RIGHTS

Reuters: **Derek Chauvin expected to change plea to guilty in George Floyd civil rights case**, Unattributed, December 15, 2021, 6:16 AM
White former Minneapolis police officer Derek Chauvin is expected to plead guilty on Wednesday in a federal court in Minnesota to charges that he violated George Floyd's civil rights during the Black man's murder, reversing his not-guilty plea in September. [Continue Reading]

AP: **Landlord accused of demanding sex from tenants to pay $4.5M**, David Porter, December 14, 2021, 7:00 PM
A landlord accused of demanding sex from his low-income tenants under threat of eviction or in exchange for helping them receive rent assistance will pay more than $4 million to settle a federal lawsuit, the

Department of Justice announced Tuesday. The action against Joseph Centanni resolves a lawsuit filed in August 2020 that accused Centanni of engaging in "severe or pervasive sexual harassment" over a period of approximately 15 years. The settlement still must be approved by a federal judge. [Continue Reading] **See also:** CNN, The Hill, McClatchy, NBC, News 12 (Brooklyn, NY), Newsweek, NJ Advance Media, NY Post, Patch (Westfield, NJ), UPI, Washington Times, WNBC-NBC (New York, NY)

Bloomberg Law: **DOJ Weighs Proposals to Examine AI Bias in Data Collection, Use,** Andrea Vittorio, December 14, 2021, 2:35 PM
The U.S. Justice Department is weighing policy or legislative proposals to address the potential for artificial intelligence to perpetuate existing biases, according to a civil rights enforcement official. "We are also reviewing whether guidance on artificial intelligence fairness and use may be necessary and effective," Kristen Clarke, assistant attorney general for civil rights, said Tuesday during an event held by the National Telecommunications and Information Administration. [Continue Reading]

Baltimore Sun: **Federal court rules Maryland violated Christian school's rights by banning it from voucher program**, Taylor Deville and Alex Mann, December 14, 2021, 5:07 PM
A federal court has ruled that Maryland violated the First Amendment rights of a private Christian school in Savage when it excluded its students from a taxpayer-funded voucher program. The suit brought by Bethel Christian Academy in Howard County against Maryland was being watched by legal experts for its national implications for state voucher programs, anti-discrimination laws and religious rights. [Continue Reading]

CIVIL LAW

AP: **Wisconsin attorney general won't enforce any abortion ban**, Scott Bauer, December 14, 2021, 5:23 PM
Wisconsin's Democratic Attorney General Josh Kaul said in an interview Tuesday that he would not investigate or prosecute anyone for having an abortion should the U.S. Supreme Court overturn Roe v. Wade and a currently unenforceable state ban takes effect. The comments to The Associated Press are Kaul's strongest to date about how he would react to the Supreme Court undoing the landmark 1973 ruling that legalized abortion nationwide. A Wisconsin ban enacted in 1849 has been unenforceable under Roe v. Wade, but would take effect again if conservative Supreme Court justices decide to overrule Roe, as they suggested during oral arguments this month in a case over Mississippi's 15-week ban on abortions. [Continue Reading]

NYT: **Judge Dismisses Trump Suit Seeking to Stop Congress From Seeing His Taxes,** Charlie Savage, December 14, 2021, 6:52 PM
A federal judge on Tuesday dismissed a lawsuit by Donald J. Trump that sought to block Congress from obtaining his tax returns, ruling that the law gives a House committee chairman broad authority to request them despite Mr. Trump's status as a former president. In a 45-page opinion, Judge Trevor N. McFadden of the Federal District Court for the District of Columbia, held that the Treasury Department can provide the tax returns to the House Ways and Means Committee, which can publish them. [Continue Reading] **See also:** CNN, The Hill, NBC, Politico, WaPo

IMMIGRATION & BORDER SECURITY

Washington Times: **Illegal immigrant Russians nabbed making run at U.S. border**, Stephan Dinan, December 14, 2021, 3:00 PM
Three vehicles piled with Russian illegal immigrants made a run at the U.S. border on Sunday, drawing gunfire from a Homeland Security officer. A Mercedes and a Ford SUV rushed toward the San Ysidro border crossing at a high rate of speed, and a Customs and Border Protection officer who was walking among the cars awaiting entry fired at the Mercedes, the government said. The bullets didn't wound

anyone, but the Mercedes crashed into the Ford and two people in the Mercedes were injured, CBP said Tuesday. Officers found 18 Russians among the two vehicles. [Continue Reading]

KFOX-Fox (El Paso, TX): **CBP seizes 714 pounds of meth, 660 pounds of marijuana at El Paso ports of entry**, Erika Esquivel, December 14, 2021, 9:12 PM
Officers with the U.S. Customs and Border Protection seized 714 pounds of methamphetamine, 105 pounds of fentanyl, 32 pounds of heroin and 660 of marijuana throughout December at different ports of entry. On Dec. 2, at the Ysleta port of entry, CBP officers intercepted a mixed load of more than eight pounds of fentanyl, seven pounds of heroin and five pounds of cocaine. The driver was an 18-year-old man, a U.S. citizen, driving a Nissan Sentra. [Continue Reading]

ANTITRUST

Law360: **DOJ, Penguin-Simon & Schuster Expect Short, In-Person Trial,** Bryan Koenig, December 14, 2021, 6:43 PM
The U. S. Department of Justice's challenge to Penguin Random House LLC's $2. 18 billion bid to buy Simon & Schuster is expected to take less than a month, the parties told a D. C. federal judge Tuesday, while eyeing in-person proceedings for the August 2022 trial. During a status conference held remotely on Tuesday, DOJ attorney John R. Read said he expects the trial to take roughly two weeks. "I tend to agree," said Daniel M. Petrocelli of O'Melveny & Myers LLP, an attorney for Penguin. [Continue Reading]

Law360: **DOJ, States Defend Challenge Of American-JetBlue Alliance,** Matthew Perlman, December 14, 2021, 6:10 PM
Enforcers hit back against a bid from American Airlines and JetBlue to duck a case challenging their regional alliance in the Northeast, telling a Massachusetts federal court it doesn't have to wait until after consumers are harmed to block the pact. The U. S. Department of Justice and a contingent of state-level attorneys general filed a response Monday to a dismissal bid from the airlines, saying the companies are arguing the court is "powerless" to prevent an antitrust violation and can only intervene after consumers are already harmed. [Continue Reading]

ENVIRONMENT

Reuters: **DOJ lawyer vows to charge more corporate execs for environmental crimes,** Sebastien Malo, December 14, 2021, 4:01 PM
The Department of Justice's new top environmental lawyer, Todd Kim, will emphasize prosecuting individuals who commit corporate environmental crimes, according to prepared remarks of a Tuesday speech before the American Bar Association. "Only individuals can go to jail, and we have found that criminal corporate accountability starts with accountability for individuals responsible for criminal conduct," said Kim, who took over the DOJ's Environment and Natural Resources Division in July. [Continue Reading]

TAX

Law360: **Ex-Illinois Rep. Pleads Guilty To Tax Evasion**, Celeste Bott, December 14, 2021, 7:00 PM
Former Illinois Rep. Edward "Eddie" Acevedo pled guilty Tuesday to a tax evasion charge after admitting in a plea agreement that he underreported and concealed the true source of his income [...] [Continue Reading] **See also:** Chicago Sun Times, Chicago Tribune

New Jersey Advance Media: **Former N.J. Dem party leader, attorney sentenced for $250K tax evasion**, Noah Cohen, December 14, 2021, 8:15 PM
A one-time Cumberland County elected official and former Democratic party leader was sentenced

Tuesday to 14 months in prison for evading more than $250,000 in federal taxes on income from his law firm, officials said. Douglas M. Long pleaded guilty last year in federal court in Camden to one count of federal income tax evasion, according to the U.S. Attorney's Office. A judge also sentenced Long to three years of supervised release, a $10,000 fine and ordered him to pay restitution of $269,736. [Continue Reading]

FEDERAL LAW ENFORCEMENT AGENCIES

CNN: **Six FBI agents investigated for allegedly soliciting prostitution while on assignment overseas,** Christina Carrega, December 14, 2021, 3:23 PM
Six FBI agents were investigated for allegedly soliciting prostitution, trafficking drugs and failing to report unofficial interactions for foreign nationals while on assignment overseas, a Justice Department watchdog says. The Justice Department's Office of the Inspector General released an investigative report on Tuesday that accuses four FBI officials of soliciting, procuring and accepting sex from prostitutes while on duty in a foreign country and lying about it. [Continue Reading] **See also:** Daily Wire, Fox, Washington Times

Dallas Morning News: **Dallas police, sheriff haven't participated in FBI use-of-force database facing possible shut-down,** Kelli Smith, December 14, 2021, 2:52 PM
Dallas police and the county sheriff's office are among enrolled North Texas law enforcement agencies that haven't provided the FBI use-of-force data for the bureau's nationwide tracker, which faces a possible shut-down because of lack of participation. [Continue Reading]

WDIV-NBC (Detroit, MI): **Detroit's Operation Holiday Wrap nets 70 felony arrests, 20+ illegal gun seizures and 35 grams of cocaine,** Victor Williams, December 14, 2021, 6:26 PM
A joint operation between Detroit police, U.S. Marshals and the ATF netted 70 felony arrests, the seizure of more than 20 illegal guns and the discovery of 35 grams of cocaine. Operation Holiday Wrap ran from Dec. 7 through Dec. 9. During that time Detroit police officers from the 5th, 9th and 11th precincts worked with the U.S. Marshals and the ATF. "The operation led to the arrest of a suspect who was wanted for murder, another suspect who was wanted for rape and five robbery suspects were also arrested," Detroit police Chief James White said. [Continue Reading]

CRIMINAL JUSTICE/CORRECTIONS

Tulsa World (Tulsa, OK): **Feds won't seek death penalty for Broken Arrow double homicide,** Curtis Killman, December 14, 2021, 3:42 PM
Federal prosecutors will not be seeking the death penalty against two men accused of a double murder in a Broken Arrow park. The decision was made public in court papers filed Monday in the case of Denim Lee Blount, 19, and Hunter Isaiah Hobbs, 20. The word came in a one-sentence letter from U.S. Attorney General Merrick Garland, who directed Acting U.S. Attorney Clint Johnson not to seek the death penalty. [Continue Reading]

CBS: **She's one of 18,000 people waiting for a presidential pardon. She knows an answer may take years.,** Clare Hymes, December 14, 2021, 11:30 AM
Sarah Carlson has been on a decade-long path to redemption since her arrest in 2009. Recently, she bought her first home, completed an internship in addiction counseling, and will soon work toward a degree in social work. But Carlson has encountered several roadblocks along the way. The Minnesota resident often struggled to secure both housing and work. As a convicted felon, Carlson had to apply for an exemption with the state to work with vulnerable adults with addiction — she had to prove her crime was nonviolent. [Continue Reading]

US SUPREME COURT

AP: **Justices asked to let Arizona enforce ban on some abortions**, Unattributed, December 14, 2021, 3:00 PM
Arizona asked the Supreme Court Tuesday to allow enforcement of a ban on abortions performed solely because of Down syndrome and other genetic abnormalities. The request from the state's Republican attorney general, Mark Brnovich, comes as the high court is weighing rolling back abortion rights nationwide and in the immediate aftermath of a decision keeping in place Texas' ban on abortion after about six weeks, while allowing some challenges to the law to continue. [Continue Reading] **See also:** Reuters, SCOTUSblog, WaPo

CNN: **Texas abortion clinics ask Supreme Court to speed up paperwork so appeals process can continue**, Ariane de Vogue, December 14, 2021, 5:00 PM
In the latest attempt to move forward with a lawsuit to block enforcement of Texas' six-week abortion ban, lawyers for abortion providers asked the Supreme Court on Tuesday to immediately transfer a certified copy of its decision from last week back to a district court judge in order to restart proceedings in short order. Although the Supreme Court last Friday allowed the controversial law to remain on the books, it did clear a narrow path for providers to try to sue a small subset of Texas licensing officials to try to block enforcement. [Continue Reading]

US ATTORNEYS

WCIA-CBS (Champaign, IL): **First black U.S. Attorney for Central Illinois on the job**, Tim Ditman, December 14, 2021, 5:55 PM
With a raise of his hand and a few words this week, the new top federal prosecutor for Central Illinois made history. Gregory K. Harris was sworn in Monday as U.S. Attorney for the Central District of Illinois, becoming the first Black person to hold that post. The swearing-in happened at the Davenport, Iowa, federal courthouse because the Rock Island, Illinois, courthouse is closed due to construction on a new courthouse. [Continue Reading]

JUDICIAL NOMINEES & APPOINTMENTS

Reuters: **Biden gets three seats to fill on 4th, 6th Circuits as judges take senior status**, Nate Raymond, December 14, 2021, 2:05 PM
President Joe Biden will have three more appellate court vacancies to fill in the new year after a trio of judges on the 4th and 6th U.S. Circuit Court of Appeals announced plans to step down from active service. The decisions by U.S. Circuit Judges Diana Gribbon Motz of the Richmond, Virginia-based 4th U.S. Circuit and Helene White and R. Guy Cole of the Cincinnati, Ohio-based 6th Circuit to take senior status were confirmed by judicial officials on Tuesday. [Continue Reading] **See also:** Law360

HuffPost: **Senate Confirms First Korean American Woman As U.S. Appeals Court Judge**, Jennifer Bendery, December 14, 2021, 2:23 PM
The Senate voted Monday night to confirm Lucy Koh to a lifetime seat on the U.S. Court of Appeals for the 9th Circuit, making her the first Korean American woman to ever serve as a federal appeals court judge. The Senate confirmed Koh in a 50-45 vote. Every Democrat voted for her. Every Republican present voted against her. Five Republicans missed the vote. [Continue Reading]

NATIVE AMERICAN AFFAIRS

KTMF-ABC/Fox (Missoula, MT): **Browning man sentenced for raping children on Blackfeet Indian Reservation**, Unattributed, December 14, 2021, 7:00 PM
A Browning man was sentenced to 15 years in prison to be followed by a lifetime of supervised release after admitting to repeatedly raping two children on the Blackfeet Indian Reservation, U.S. Attorney Leif

M. Johnson said. Jonathan Cadotte, 60, pleaded guilty in August to a superseding information charging him with aggravated sexual abuse and to aggravated sexual abuse of a child. [Continue Reading] **See also**: KECI-NBC (Missoula, MT), KRTV-CBS (Great Falls, MT)

CONGRESS

Fox: **Sen. Ron Johnson asks DOJ if it tracks criminal record of accused felons granted pre-trial release,** Michael Lee , December 14, 2021, 6:10 PM
Sen. Ron Johnson, R-Wis., penned a letter to Attorney General Merrick Garland seeking information on Department of Justice efforts to monitor the trend of pre-trial releases for individuals charged with a felony. "The attack on the Waukesha Christmas Parade by a repeat violent offender brought to the nation's attention the issue of pre-trial release of criminal violent offenders and subsequent violent crimes committed by such individuals," Johnson said in the letter, which was sent Tuesday. [Continue Reading]

NETWORK EVENING NEWS LINEUP: DECEMBER 14, 2021

- A federal judge on Tuesday dismissed a lawsuit by Donald J. Trump that sought to block Congress from obtaining his tax returns, ruling that the law gives a House committee chairman broad authority to request them despite Mr. Trump's status as a former president. [NBC]
- Tonight, the House is set to vote to hold former White House Chief of Staff Mark Meadows in contempt and could lead to criminal charges for Meadows' refusal to cooperate with the investigation into the Jan. 6th attack on the capitol. [ABC, CBS, NBC]
- The US has reached yet another staggering milestone, with 800,000 Americans now confirmed lost to the coronavirus, according to newly updated data from Johns Hopkins University. A new antiviral pill from Pfizer could be the breakthrough drug in the coronavirus pandemic. The news comes as the US nears a grim new milestone of 800,000 COVID-related deaths. [ABC, CBS, NBC]
- Federal agents have sent an evidence response team to the Carnival Miracle after the cruise line said a woman in her 20s fell overboard early Saturday morning. [ABC]
- Andrew Cuomo must return millions of dollars in proceeds from a memoir published while he was governor of New York, a state ethics panel voted Tuesday. Members of the Joint Commission on Public Ethics voted 12-1 for a resolution giving Cuomo 30 days to turn the money over to the New York State Attorney General. [CBS]
- Inside Look At Retail Theft Sting. In Perrysburg Township, Ohio, where a team of detectives respond daily to organized retail crime and track stolen goods online. The goods often end up on Facebook Marketplace. In a statement, a Facebook spokesperson says in part, "We prohibit the sale of stolen goods on our platform and use a number of tools to prevent this kind of fraud." [NBC]

From: Coley, Anthony D. (PAO)
Subject: Abbreviated Weekend Clips
To: Klapper, Matthew B. (OAG)
Cc: Iverson, Dena (PAO); Heinzelman, Kate (OAG); Goodlander, Margaret V. (OAG); Matthews-Johnson, Tamarra D. (OAG); Visser, Tim (OAG); Reich, Mitchell (OAG)
Sent: December 12, 2021 2:50 PM (UTC-05:00)

AFTERNOON HEADLINES

- "In response to Texas abortion ban, Newsom calls for similar restrictions on assault weapons" [LAT]
- "Death toll expected to rise as recovery effort continues" [WaPo, WSJ, NYT]

NATIONAL SECURITY

AP: **UK opens door to Assange extradition to US on spying charges,** Danica Kirka and Jill Lawless, December 10, 2021, 1:00 PM
A British appellate court opened the door Friday for Julian Assange to be extradited to the United States on spying charges by overturning a lower court decision that the WikiLeaks founder's mental health was too fragile to withstand incarceration in America. The High Court in London ruled that U.S. assurances about Assange's detention, received after the lower court decision, were enough to guarantee he would be treated humanely. Assange's lawyers say they will ask to appeal. [Continue Reading] **See also:** NYT, WaPo

Fox: **ISIS propaganda figure pleads guilty in US court to aiding terrorist group,** Caitlin McFall, December 11, 2021, 3:00 PM
A Saudi-born Canadian citizen who joined the Islamic State nearly a decade ago pleaded guilty Friday after serving as one of the terrorist group's leading propagandists. Mohammed Khalifa, 38, pleaded guilty to "conspiring to provide material support or resources to a foreign terrorist organization, resulting in death" at a hearing at the U.S. District Court in Alexandria, Virginia. [Continue Reading] **See also:** The Hill

Law360: **DOJ's China Initiative On Trial As Harvard Prof. Faces Jury,** Unattributed, December 10, 2021, 4:16 PM (EST)
A renowned Harvard University nanotechnology professor will stand trial starting Tuesday for allegedly hiding his ties to the Chinese government in what experts say will be a high-profile test for the…[Continue Reading]

Law360: **Corruption, Cybercrime In Crosshairs For DOJ Crime Chief,** Unattributed, December 10, 2021, 3:56 PM (EST)
The Biden administration has deemed global corruption a key national security threat, marshaling the full power of the federal government to combat the flow of dirty money. Cybercrime enforcement is a… [Continue Reading]

Pittsburgh Post-Gazette (Pittsburgh, PA): **Rising cyber ransom attacks costing Pennsylvania victims millions,** Jonathan D. Silver and Joel Jacobs, December 12, 2021, 6:00 AM
For Tops Staffing, a suburban Pittsburgh company with workers across the nation, the cyber attack shook the business like few other events. [...] The company contacted the FBI and scrambled to get back online. Susan C. Dietrich, the principal owner and president, called the situation "one hell of a problem." [Continue Reading]

JAN. 6

CNN: **Judge upholds prosecutors' use of felony obstruction law in January 6 cases in pivotal**

ruling, Marshall Cohen and Hannah Rabinowitz, December 10, 2021, 8:22 PM
A federal judge on Friday upheld the Justice Department's decision to use a felony obstruction law against US Capitol rioters, a major victory for prosecutors who have used the statute to charge hundreds of Donald Trump supporters who were involved in the January 6 insurrection. Several other defendants have challenged the law, and many of those challenges are still pending. But Friday's ruling means the Justice Department's strategy for charging the Capitol rioters has survived a key test. [Continue Reading]

Reuters: **U.S. House Capitol Jan. 6 probe subpoenas more Trump aides,** Patricia Zengerle, December 10, 2021, 4:35 PM (EST)
The U.S. House of Representatives committee probing the deadly Jan. 6 Capitol riot said on Friday it had issued six more subpoenas demanding information from witnesses, including some top aides from former President Donald Trump's White House. The House of Representatives Select Committee issued subpoenas to Brian Jack, who was Trump's White House political director; Max Miller, a former special assistant to Trump now running for a House seat in Ohio with Trump's endorsement; and Bobby Peede, former director of the White House advance staff, which prepared events for Trump's arrival. [Continue Reading] **See also:** CNN, WaPo

Reuters: **California man charged in Jan. 6 U.S. Capitol riot flees to Belarus,** Mark Hosenball and Steve Gorman, December 10, 2021, 9:25 PM (EST)
A California man charged with assaulting police in the Jan. 6 riot at the U.S. Capitol and using a metal barricade as a battering ram has fled the United States and is believed to have taken refuge in Belarus, federal prosecutors said on Friday. Evan Neumann, 49, was indicted on Friday on 14 criminal counts stemming from the deadly Capitol siege by supporters of then-President Donald Trump, expanding on charges originally contained in a criminal complaint filed against Neumann in March. [Continue Reading]

CNN: **After 50 rioters sentenced for January 6 insurrection, a debate rages over what justice looks like,** Marshall Cohen, December 11, 2021, 8:06 AM
Of the 50-plus defendants who have been sentenced for their role in the January 6 attack on the US Capitol, fewer than half were sent to jail for their crimes. Most received an assortment of lesser penalties, including brief terms of house arrest, a couple years of probation, four-figure fines or court-ordered community service, according to a CNN analysis. The milestone of 50 sentencings was hit on Friday, a busy day in court, with six hearings on the schedule. [Continue Reading]

AP: **Capitol rioters' social media posts influencing sentencings,** Michael Kunzelman, December 11, 2021, 10:28 PM (EST)
For many rioters who stormed the U.S. Capitol on Jan. 6, self-incriminating messages, photos and videos that they broadcast on social media before, during and after the insurrection are influencing even their criminal sentences. Earlier this month, U.S. District Judge Amy Jackson read aloud some of Russell Peterson's posts about the riot before she sentenced the Pennsylvania man to 30 days imprisonment. "Overall I had fun lol," Peterson posted on Facebook. [Continue Reading]

USA Today: **Capitol riot misinformation persists: False claims continue to circulate on Facebook,** Daniel Funke, December 10, 2021, 1:50 PM (EST)
Months after supporters of now-former President Donald Trump stormed the U.S. Capitol, debunked conspiracy theories about who was behind the insurrection continue to circulate on Facebook. That's according to new research from Avaaz, shared exclusively with USA TODAY. [Continue Reading]

Bloomberg: **Bannon Restricted From Publicizing DOJ Evidence in Contempt Case,** Erik Larson, December 11, 2021, 2:03 AM
A federal judge placed limits on how former Trump campaign chairman Steve Bannon can use information handed over by the U.S. Justice Department in the criminal case over his refusal to

cooperate with a congressional probe into Jan. 6 Capitol riot. U.S. District Judge Carl Nichols in Washington on Friday granted most of what federal prosecutors asked for in a so-called protective order they sought for internal records from the House select committee probing the assault. [Continue Reading]

WUSA-CBS (Washington, D.C): **Despite 'inspiring' immigrant story, former Houston Police officer gets 45 days in jail for Capitol riot,** Eric Flack, Jordan Fischer, and Stephanie Wilson, December 10, 2021, 9:03 PM (EST)
In what appeared to be a very close call for a federal judge, former Houston Police Officer Tam Dinh Pham was sentenced to 45 days in prison Friday for his conviction on a misdemeanor charge from the January 6 Capitol riot. “You added an air of legitimacy to what happened that day because you are a police officer,” U.S. District Judge Timothy Kelley told Pham. [Continue Reading] **See also:** KRIV-Fox (Houston, TX)

CRIMINAL LAW

AP: **Prosecution rests in sex-abuse trial of Ghislaine Maxwell,** Larry Neumeister and Tom Hays, December 10, 2021, 4:51 PM (EST)
Prosecutors completed presenting their case against Ghislaine Maxwell on Friday, after a key accuser at the British socialite’s sex-abuse trial testified that Maxwell and her companion, Jeffrey Epstein, forced themselves on her when she was just 16. [...] U.S. District Judge Alison J. Nathan heard brief arguments and rejected the request that she acquit Maxwell without the jury ever getting the case. [Continue Reading] **See also:** CNN, Fox, NPR, NYT, Reuters, WSJ, WaPo

CNN: **CNN Producer John Griffin arrested for attempting to persuade minors to engage in unlawful sexual activity,** Christina Maxouris, December 11, 2021, 6:57 PM (EST)
Connecticut man John Griffin was arrested Friday and charged with three counts of using a facility of interstate commerce to attempt to entice minors to engage in unlawful sexual activity, the United States Attorney's Office for the District of Vermont said in a news release. Griffin, 44, has been a producer with CNN for about eight years. [Continue Reading] **See also:** The Hill, NY Daily News, WVIT-NBC (New Britain, CT)

The Hill: **Former NFL player given three-year prison sentence for pandemic relief fraud,** Lexi Lonas, December 10, 2021, 7:53 PM (EST)
A former NFL player was sentenced to three years in prison for pandemic relief fraud, the Department of Justice (DOJ) announced Friday. The DOJ said 32-year-old Joshua J. Bellamy will spend 37 months in prison for fraudulently getting a $1.2 million Paycheck Protection Program (PPP) loan. [Continue Reading] **See also:** KSWB-Fox (San Diego, CA), Law360, Louisville Courier-Journal (Louisville, KY),, Patch (St. Pete, FL), Tampa Bay Times (St. Petersburg, FL), WTSP-CBS (St. Petersburg, FL),

NYT: **Ex-Panama President’s Sons Are Extradited to U.S. After Multicountry Chase,** Mike Ives, December 11, 2021, 4:06 AM
A Brooklyn court plans to arraign the son of a former Panamanian president on money-laundering charges on Saturday, the result of an extradition case that according to prosecutors featured a stealth getaway to the Bahamas, fake diplomatic credentials and a private jet idling on a tarmac in Guatemala. The defendant, Ricardo Alberto Martinelli Linares, was captured in Guatemala last year with his brother and indicted in February. He was extradited to the United States on Friday and will face charges in U.S. District Court in Brooklyn, prosecutors say. [Continue Reading]

AP: **Former Long Island prosecutor begins prison sentence,** Unattributed, December 11, 2021, 12:15 PM

A former Long Island prosecutor convicted of obstructing justice after a prisoner was beaten has begun serving a five-year federal prison sentence. Former Suffolk County District Attorney Thomas Spota and a former top aide, Christopher McPartland, surrendered at separate federal prisons Friday, prison officials told Newsday. Spota and McPartland were convicted in December 2019 on counts of conspiracy, obstruction of justice, witness tampering and civil rights violations. [Continue Reading]

Law360: **DOJ Levies Rare Commodities-Based Insider Trading Charges,** Al Barbarino, December 10, 2021, 8:31 PM
The U. S. Department of Justice announced rare criminal charges related to insider trading in commodities markets on Friday, claiming a Puerto Rico-based trader relied on material nonpublic information about the natural gas markets to enter fictitious, noncompetitive futures trades and gain illegal profits. Between approximately August 2015 and December 2018, Peter Miller entered fraudulent, noncompetitive trades that caused prices to "be reported, recorded, and registered on the exchanges that were not true, bona fide prices," then split the profits with his co-conspirators, the DOJ said in an indictment filed this week. [Continue Reading]

Law360: **DOJ May Face Hurdles In Individual Wire Fraud Prosecutions,** Unattributed, December 10, 2021, 2:45 PM (EST)
The U.S. Department of Justice's announcement that its single most important white collar imperative is the prosecution of individuals raises the question of whether it even has jurisdiction to convict most… [Continue Reading]

CIVIL RIGHTS

LAT: **This isn't the first time Torrance Police Department has been accused of widespread racism,** James Queally, December 10, 2021, 6:03 PM (EST)
When Torrance police officers saw Black people in their city in the 1990s, they had two special phrases to describe them, according to a federal lawsuit. A pair of acronyms — "NIT" and "NITAD" — both used a racial slur to note that a Black person was either "in Torrance" or "in Torrance after dark," according to the testimony of former Torrance police officers contained in U.S. Department of Justice filings. [Continue Reading]

Law360: **Ga. Judge Keeps Alive DOJ Suit Against State Voting Law,** Unattributed, December 10, 2021, 5:31 PM (EST)
The U.S. Department of Justice can continue its challenge of a controversial Georgia voting law enacted in March after a Georgia federal judge found that officials have plausibly claimed that the…[Continue Reading]

Chicago Sun-Times: **The Emmett Till case is closed, but the fight for justice against racial violence continues,** Christopher D. Benson, December 11, 2021, 5:00 AM (EST)
For more than 66 years, the family of Emmett Till has asked who would answer for his brutal 1955 lynching in the Mississippi Delta. This past week, they got the response. No one will answer for Emmett's death. No one will be brought to justice. [Continue Reading]

Atlanta Black Star: **Justice Department Continues to Look at 20 Cold Cases from the Civil Rights Era; 13 of Which Are Police-Involved Killings In Southern States,** Nicole Duncan-Smith, December 11, 2021, 6:51 PM
This week the United States Justice Department closed its investigation into the death of Emmett Till. Despite finding no new evidence to bring new charges in the 14-year-old's 1955 lynching, the FBI's Cold Case Initiative continues to investigate other cold-case crimes with racial bias implications from the civil rights movement era. The Justice Department Cold Case Initiative was founded by the FBI in 2006. [Continue Reading]

KXAN-NBC (Austin, TX): **State of Texas: Federal lawsuit over redistricting might delay Texas primary election,** Tahera Rahman, Monica Madden, Will DuPree, and Sandra Sanchez, December 12, 2021, 7:00 AM (EST)
The U.S. Department of Justice is suing the state of Texas, saying the state's new redistricting maps deny and dilute votes from people of color. The DOJ says Texas' new maps purposely violate Section 2 of the federal Voting Rights Act based on certain voters' race and/or minority group — also known as "vote dilution." [Continue Reading]

CIVIL LAW

Reuters: **Group wins new chance to obtain Yates' DOJ emails over Trump travel ban,** Nate Raymond, December 10, 2021, 5:04 PM (EST)
A federal appeals court on Friday overturned a decision allowing the U.S. Justice Department to withhold records concerning former Acting U.S. Attorney General Sally Yates' 2017 refusal to defend then-President Donald Trump's travel ban targeting seven Muslim-majority nations. The U.S. Court of Appeals for the District of Columbia Circuit gave the conservative group Judicial Watch a new shot at winning the release of drafts of a Jan. 30, 2017, statement by Yates directing officials to not defend Trump's executive order. [Continue Reading]

WaPo: **[OPINION] Distinguished persons of the week: The D.C. Circuit shuts down Trump,** Jennifer Rubin, December 12, 2021, 7:45 AM
The Supreme Court may have lost its luster due to its blatant partisanship, but lower federal court judges are consistently upholding the Constitution and not allowing Jan. 6 to go down the memory hole. The three-judge U.S. Court of Appeals for the D.C. Circuit on Thursday issued a unanimous opinion shutting down former president Donald Trump's ludicrous claim that he can assert executive privilege over White House documents in contravention of the current president's waiver of privilege claims. [Continue Reading]

IMMIGRATION & BORDER SECURITY

Reuters: **U.S. to coordinate with Mexico, regional countries for crackdown on people smuggling,** Unattributed, December 11, 2021, 9:39 PM (EST)
The United States, Mexico and several regional countries will coordinate to apprehend the network of human smugglers responsible for a deadly accident that killed dozens of migrants, the U.S. embassy in Mexico said on Saturday. The embassy announced the creation of an action group tasked with investigating, identifying and apprehending the smugglers involved in organizing a trailer, crammed with more than 160 people, which overturned on Thursday in the Mexican state of Chiapas. [Continue Reading]

Law360: **Garland To Review Mental Health In Migrant Crime Cases,** Unattributed, December 10, 2021, 4:53 PM (EST)
Attorney General Merrick Garland will review a 2014 ruling preventing immigration courts from considering whether a noncitizen's mental health history lightens the immigration consequences of a conviction, according to a notice…[Continue Reading]

Yahoo News: **Operation Whistle Pig: Inside the secret CBP unit with no rules that investigates Americans,** Jana Winter, December 11, 2021, 4:00 AM
It was almost 10 p.m. on a Thursday night, and Ali Watkins was walking around the capital following instructions texted by a stranger. One message instructed her to walk through an abandoned parking lot near Washington, D.C.'s Dupont Circle, and then wait at a laundromat. Then came a final cryptic instruction: She was to enter an unmarked door on Connecticut Avenue leading to a hidden bar.

[Continue Reading]

USA Today: **Dangerous wait for freedom: Hurdles abound for transgender migrants seeking asylum in US,** Rebecca Morin, December 12, 2021, 6:00 AM (EST)
Regina King just wanted to be herself. But in her home country of Guyana, it was difficult. [...] On the U.S. side, some advocates also warn that transgender individuals are often misgendered when taken into Customs and Border Protection custody or Immigration and Customs Enforcement custody, which could lead to attacks from other inmates while in custody due to their gender identity or neglect from DHS officials. [Continue Reading]

NYT: **Helicopters and High-Speed Chases: Inside Texas' Push to Arrest Migrants,** J. David Goodman, December 11, 2021, 9:23 PM (EST)
Magdaleno Ruiz Jimenez huddled under a waxing moon in the rough brush of a Texas ranch. His journey to the small border community of Brackettville had been long, about 1,300 miles from his home in Mexico. [...] Representative Joaquin Castro, a San Antonio Democrat, has asked for a federal investigation of the Operation Lone Star, saying in a letter this fall to the Justice Department that the program was "wreaking havoc on Texas' judicial system" and has "directly led to a violation of state laws and constitutional due process rights."[Continue Reading]

ANTITRUST

Reuters: **Cemex says U.S. Justice Dept. closed anti-trust investigation,** Unattributed, December 10, 2021, 9:08 PM (EST)
Mexico's Cemex, one of the world's largest cement companies, said Friday that the U.S. Department of Justice (DOJ) has closed an investigation against the company for a possible violation of anti-trust laws. Cemex (CEMEXCPO.MX) also reported that it was fined about 68 million euros ($77 million) by Spanish authorities following tax audits of its operations from 2010 to 2014. [Continue Reading]

FEDERAL LAW ENFORCEMENT AGENCIES

CNN: **More than 300 arrested by US Marshals in Gulf Coast crime sweep targeting violent criminals,** Nadeem Muaddi, December 11, 2021, 4:01 AM (EST)
The US Marshals Service announced the end of a 26-long-week, multiagency crime sweep, resulting in the arrest of more than 350 people on the Gulf Coast. The action, dubbed "Operation Triple Beam - Third Coast," targeted documented gang members and violent offenders, and sought to identify targets and collect criminal intelligence, the US Marshals said in a statement on Monday. [Continue Reading]

CNN: **Fueled by gun violence, cities across the US are breaking all-time homicide records this year,** Priya Krishnakumar, December 12, 2021, 8:33 AM
One of the fastest-growing cities in the country, the capital of Texas is nearing the end of its deadliest year on record in 2021 as cities nationwide are experiencing a rise in homicides and gun violence incidents that began last year when the pandemic tightened its grip on the US. Fueled by what both authorities and community leaders say is the easy access to guns, Austin has recorded 88 homicides so far this year, shattering the previous high of 59 in 1984. [Continue Reading]

Fox: **New Orleans homicide rate reaches 14-year high following fatal shooting near hotel,** Kyle Morris, December 11, 2021, 6:52 PM (EST)
A man was fatally shot on Friday in New Orleans, marking the city's 201st homicide of the year, a 14-year high in the total number of homicides in Louisiana's most populous city. [...] The 201st homicide matched the city's 2020 homicide record. Prior to 2020, that number had not been reached since 2007, according to FBI records. [Continue Reading]

Politico: **Fortenberry indictment raises questions about the FBI's tactics,** Josh Gerstein, December 12, 2021, 7:00 AM (EST)
The Justice Department's prosecution of a Republican lawmaker for allegedly lying to the FBI is raising thorny issues about the use of surreptitious tactics during investigations into members of Congress. The false-statement indictment brought against Rep. Jeff Fortenberry of Nebraska two months ago is also resurfacing many of the same questions that triggered a firestorm of controversy around the prosecution of former national Security Adviser Michael Flynn. [Continue Reading]

CRIMINAL JUSTICE/CORRECTIONS

NPR: **Activists wanted Biden to revamp the justice system. Many say they're still waiting,** Carrie Johnson, December 12, 2021, 5:00 AM
[...] The advocates say they're happy to give credit where it's due. They praised the Justice Department for rescinding a Trump-era memo that directed prosecutors to pursue the most serious charges they could for any crime. [...] But they've also taken note of this fact: the federal prison population has increased by some 5,000 people during Biden's tenure, according to Nazgol Ghandnoosh, a researcher at the Sentencing Project. [Continue Reading]

The Star-Ledger (Newark, NJ): **Who is Jane Parnell? The powerful new monitor for N.J.'s troubled women's prison.**, Blake Nelson, December 12, 2021, 9:00 AM
[...] Jane Parnell officially became the federal monitor for the Edna Mahan Correctional Facility on Aug. 24, when a federal judge signed off on a consent decree between New Jersey and the U.S. Department of Justice. For at least the next three years, Parnell will oversee reforms to reverse years of well-documented violence and sexual abuse at the Hunterdon County prison. [Continue Reading]

US SUPREME COURT

Reuters: **U.S. Supreme Court leaves Texas abortion curbs intact but allows suit,** Lawrence Hurley and Andrew Chung, December 10, 2021, 4:14 PM (EST)
The U.S. Supreme Court on Friday left in place a ban on most abortions in Texas but allowed a legal challenge to proceed, with the fate of the Republican-backed measure that allows private citizens to enforce it still hanging in the balance. The justices in an 8-1 ruling lifted a block on lower court proceedings and permitted a lawsuit by abortion providers, which may pave the way for a federal judge to block the nation's toughest abortion law at least in part. [Continue Reading] **See also:** AP, BuzzFeed, CNN, NBC, NPR, NYT, Politico, SCOTUSblog, WSJ, WaPo

Reuters: **Biden concerned by Supreme Court decision to keep abortion curbs in Texas,** Unattributed, December 10, 2021, 3:00 PM (EST)
U.S. President Joe Biden is "very concerned" by the Supreme Court's decision to leave in place a ban on most abortions in Texas, the White House said on Friday, adding that he is deeply committed to the landmark 1973 Roe v. Wade ruling that legalized the procedure nationwide. Biden plans to issue a statement on the Supreme Court's decision later on Friday, White House press secretary Jen Psaki told reporters. [Continue Reading]

US ATTORNEYS & DOJ GRANTS

Concord Monitor (Concord, NH): **New Hampshire's first safe house for human trafficking victims will open next year,** Cassidy Jensen, December 12, 2021, 9:00 AM
A half million dollars in federal grant money will finally allow a safe house for victims of human trafficking to open, the first transitional housing of its kind in New Hampshire. Executive Director Bethany Cottrell said the three-year grant of $583,586 from the U.S. Department of Justice's Office of Justice Programs will allow Brigid's House of Hope to sign a lease on a building and hire staff to support women escaping

sex trafficking at a restorative safe house. [Continue Reading]

Ohio County Monitor (Beaver Dam, KY): **AG's Office awarded $600,000 to provide transitional housing for human trafficking survivors,** Unattributed, December 11, 2021, 1:20 PM (EST)
Attorney General Daniel Cameron today announced that his office was awarded a $600,000 federal grant from the Department of Justice to develop a transitional and short-term housing-assistance program for survivors of human trafficking. The Attorney General's Office of Trafficking and Abuse Prevention and Prosecution will develop the program in partnership with Refuge for Women, a nonprofit recovery program for survivors of human trafficking and sexual exploitation. [Continue Reading]

Muskogee Phoenix (Muskogee, OK): **Justice Department awards funding for Project Safe Neighborhoods,** Unattributed, December 10, 2021, 8:11 PM
The Department of Justice announced Thursday that it has awarded more than $17.5 million in grants to support the Project Safe Neighborhoods (PSN) Program. Funding will support efforts across the country to address violent crime, including the gun violence that is often at its core. [Continue Reading]

KVVU-Fox (Las Vegas, NV): **Henderson police to get funding to bolster opioid epidemic response,** Kristen Desilva, December 10, 2021, 3:37 PM (EST)
The Department of Justice on Friday awarded the Henderson Police Department funds to help bolster their efforts amid the opioid epidemic. The two Paul Coverdell Forensic Science Improvement Grants total $270,486. [Continue Reading]

KTVT-CBS (Fort Worth, TX): **Department Of Justice Awards Over $378K To Project Safe Neighborhoods In North Texas,** Unattributed, December 10, 2021, 1:51 PM (EST)
Today, the Department of Justice awarded more than $378,000 in North Texas to help support efforts to address violent crime. Project Safe Neighborhoods (PSN) is a national program meant to address violent crime in cities across the United States, including gun violence. It was originally launched in 2001 with support from the Bush administration. [Continue Reading]

KATC-ABC/CW+ (Lafayette, LA): **Biden nominee sworn in as U.S. Attorney for Louisiana's western district,** Unattributed, December 10, 2021, 5:57 PM (EST)
Brandon Bonaparte Brown was officially sworn in today as United States Attorney for the Western District of Louisiana. The Southern Law alumnus and Louisiana native was nominated by President Joe Biden on November 15 and was confirmed by the United States Senate on December 7. [Continue Reading]

NATIVE AMERICAN AFFAIRS

Tulsa World (Tulsa, OK): **Supreme Court sets date with Oklahoma to respond to 40-plus McGirt appeals,** Curtis Killman, December 12, 2021, 1:35 AM (EST)
The state of Oklahoma, with more than 40 petitions filed seeking to overturn or limit the McGirt ruling, is getting its shot next month after the U.S. Supreme Court last week picked a date to consider appeals related to its landmark decision. When the nine justices gather Jan. 7, a Tulsa man's case will be in the spotlight: The state appealed after the Oklahoma Court of Criminal Appeals vacated a 2017 conviction and 35-year prison sentence for Victor Manuel Castro-Huerta, 36, based on the McGirt ruling. [Continue Reading]

OPIOID CRISIS

WaPo: **In Congress, David Trone keeps it personal: Combating the opioid epidemic that killed his nephew,** Meagan Flynn, December 11, 2021, 6:53 PM
Five years after the death of his nephew, David Trone went to Mexico looking for the source of what

killed him: the opioid epidemic. It was official business — a trip last month in his capacity as co-chair of the Commission on Combating Synthetic Opioid Trafficking — but now it was hard to separate the personal from the official, as almost everything the Maryland Democrat was doing in Congress found its way back to Ian. Halfway through his second term, combating the crisis that killed his nephew has become his biggest mission in Congress. [Continue Reading]

ADMINISTRATION

WaPo: **Biden rallies the world to strengthen democracy as big challenges loom at home,** Dan Balz, December 11, 2021, 1:21 PM (EST)
President Biden gathered, virtually, representatives of more than 100 countries for what was billed as a "Summit for Democracy" on Thursday and Friday. The goal was to rally nations in the face of rising authoritarianism around the world. "Democracy needs champions," the president said. [Continue Reading]

CONGRESS

Reuters: **Former Trump adviser Navarro refuses subpoena in U.S. House coronavirus probe,** Unattributed, December 11, 2021, 6:24 PM (EST)
Former White House trade adviser Peter Navarro has refused to comply with a subpoena for documents related to the Trump administration's response to the coronavirus, saying the former president ordered him not to, according to his response to a congressional request released on Saturday. [...] Navarro, a Republican, also served as one of former President Donald Trump's pandemic response advisers and was responsible for procurement in the coronavirus response, among other things. Navarro said in a letter to the subcommittee he would not cooperate because Trump told him to "protect executive privilege." [Continue Reading] **See also:** Axios, CNN

NYT: **Some Voters Are at Odds With Their Party on Abortion,** Nate Cohn, December 11, 2021, 2:05 PM (EST)
Abortion is one of the most polarizing issues in Washington. Congressional Democrats and Republicans all but unanimously back their party's view on abortion, and many highly engaged activists feel the same way. [...] The bitterly partisan fight unfolding in statehouses and courthouses, even in the Supreme Court's split decision on Friday over the Texas abortion law, can obscure how many Americans of all parties struggle with the weighty moral and ethical questions raised by abortion. [Continue Reading]

NETWORK EVENING NEWS LINEUP: DECEMBER 10, 2021

- The Supreme Court refused to block a Texas law banning abortions for anyone more than six weeks pregnant. Separately, the Court dismissed as improvidently granted the Justice Department's challenge to the law, meaning the Court should not have accepted the case in the first place. Abortion providers in Texas, however, can challenge a state law banning most abortions after six weeks, allowing them to sue at least some state officials in federal court. [ABC, CBS, NBC]
- Violent crime rising across the country is now encroaching onto college campuses. College campuses are implementing proactive strategies, modern technology, and increasing their police force. [CBS]
- The prosecution rested its case in the trial of Ghislaine Maxwell. Prosecutors say Maxwell helped to recruit and groom teenage girls for sexual abuse by Mr. Epstein. Maxwell has pleaded not guilty, denying the accusations, her trial will continue on Thursday [CBS]
- Inflation is at a 40 year high with the November 2021 Consumer Price Index up 0.8% with prices up 6.8% compared to a year ago. President Biden acknowledged inflation is affecting many families,

pointing to COVID and the supply chain crisis while assuring the rising prices are temporary. [ABC, CBS, NBC]
- Tougher new COVID rules are being put in place as US Healthcare systems are on the brink of collapse due to the Delta surge and OMICRON variant increasing the number of hospitalizations. New York has placed a statewide mask mandate at all public places and indoor businesses. [ABC, CBS, NBC]
- Ariel Pennington allegedly assaulted a flight attendant and Air Marshall causing a flight bound for Los Angeles to be diverted to Oklahoma City. Pennington, booked into Oklahoma City Jail on complaints of disorderly conduct and public drunkenness, is also facing possible federal charges. [ABC, NBC]
- An out-of-control tractor-trailer carrying more than 160 migrants, mostly Central American migrants who were being smuggled to the U.S., crashed into a pedestrian bridge in southern Chiapas state outside the city of Tuxtla Gutiérrez. At least 55 migrants were killed and 104 injured. [ABC, NBC]
- In Washington, D.C., Senator Bob Dole's funeral took place at the Washington National Cathedral. In attendance were President Joe Biden, first lady Jill Biden, Vice President Kamala Harris, second gentleman Doug Emhoff, several Cabinet members, Former President Bill Clinton, former Vice President Dan Quayle, former Vice President Dick Cheney, former Vice President Mike Pence, and several current and former members of Congress. [ABC, CBS]
- A new police bodycam video presented in Court demonstrates former Minnesota Police Officer Kim Potter's hysterical reaction to her mistakenly shooting Daunte Wright with a gun instead of a Taser. The defense focused on the justified use of force, while the prosecution said Potter's actions endangered those around her. [ABC]

NETWORK EVENING NEWS LINEUP: DECEMBER 11, 2021

- What is likely the deadliest weather disaster in over 4 years has swept across the Nation. Storms passed through at least 6 states with at least 70 people dead and many unaccounted for. Tornados hit Kentucky, Arkansas, Missouri, Mississippi, Tennessee, and Illinois destroying everything in its path. [CBS, NBC-1, NBC-2]
- President Joe Biden stated there would be severe economic consequences In response to a possible invasion of Ukraine by Russia. Biden also spoke of the placement of US and NATO troops into the eastern flank to defend all the NATO Countries there against an attack from Russia and bolster American allies in Europe. [CBS]

SUNDAY MORNING TALK SHOWS

ABC This Week with George Stephanopoulos

- White House chief medical adviser Dr. Anthony Fauci joined Stephanopoulos to discuss "sobering news" that the Omicron COVID-19 variant can evade the initial protection vaccines give. However, boosters increase efficacy and better protect against the newest variant of concern, Dr. Fauci said Sunday. The variant can also evade protections provided by monoclonal antibodies and convalescent plasma. The White House chief medical adviser told ABC's "This Week" anchor George Stephanopoulos, so, "If you want to be optimally protected, absolutely get a booster," he said. [Watch]

NBC Meet the Press with Chuck Todd

- Secretary of State Antony Blinken joined Todd to discuss the leverage the US has if Russia decides to invade Ukraine, President Biden's reference to economic consequences against Russia, consequences the US, NATO, and G7 Countries are prepared to act on if Russia takes aggressive actions against Ukraine, and the possibility of an in-person meeting between Biden and Putin.

[Watch]

From: Coley, Anthony D. (PAO)
Subject: Abbreviated AM Clips
To: Klapper, Matthew B. (OAG)
Cc: Iverson, Dena (PAO); Heinzelman, Kate (OAG); Seidman, Ricki (OASG); Matthews-Johnson, Tamarra D. (OAG); Goodlander, Margaret V. (OAG); Visser, Tim (OAG); Reich, Mitchell (OAG)
Sent: October 19, 2021 7:51 AM (UTC-04:00)

MORNING HEADLINES

- "'Don't feel sorry for me,' Powell said as the end approached" [WaPo, LAT]
- "Lawmakers Step Up Pressure to Adopt Tougher Tech Laws" [WSJ]
- "Mark Ridley-Thomas will 'step back' from council duties, but not resign" [LAT]

US DEPARTMENT OF JUSTICE NEWS

AP: **Justice Department asks Supreme Court to pause Texas abortion law,** Mark Sherman, October 18, 2021, 4:56 PM
The Biden administration is asking the Supreme Court to block the Texas law banning most abortions, while the fight over the measure's constitutionality plays out in the courts. The administration also took the unusual step of telling the justices they could grant the Texas law full review and decide its fate this term, which already includes a major case about the future of abortion rights in the U.S. [Continue Reading] **See also:** Bloomberg, CBS, CNBC, CNN, Independent, LAT, Law360, NBC, NYT, Politico, Reuters, SCOTUSblog, The Texas Tribune, USA Today, WaPo, Washington Times, WSJ

NATIONAL SECURITY

Newsweek: **Capitol Rioter Who Tased Officer Fanone Suggests He 'Acted on Behalf' of Donald Trump,** Aila Slisco, October 18, 2021, 6:29 PM
A man accused of tasing Washington, D.C Police Officer Michael Fanone during the riot at the U.S. Capitol on January 6 may defend himself in court by claiming that he was acting "on behalf of" former President Donald Trump. Lawyers for defendant Daniel Rodriguez indicated that their client "may" choose to employ the "public authority defense," according to court documents filed on Friday and obtained by Law & Crime. A required legal notice lists "The Executive Branch" as "the law enforcement agency or federal intelligence agency involved" and Trump as "the agency member on whose behalf the defendant claims to have acted." [Continue Reading]

BuzzFeed: **New Capitol Surveillance Footage Shows A Breach By Jan. 6 Rioters From Start To Finish,** Zoe Tillman, October 18, 2021, 10:00 AM
A pair of US Capitol surveillance videos disclosed last week by prosecutors offer a new perspective into how a mob overwhelmed police officers and repeatedly breached a main access point to the building during the Jan. 6 riots. The footage shows a small team of US Capitol Police officers vastly outnumbered by the crush of people trying to get in. There are at most five officers in the frame at any given moment; hundreds of people flow through that entry point on the Upper West Terrace of the Capitol over the span of roughly 13 minutes. [Continue Reading]

WRC-NBC (Washington, DC): **US Marshals Inspect DC Jail, Interview Capitol Insurrection Inmates,** Scott MacFarlane, October 18, 2021, 6:00 PM
U.S. marshals are inspecting the D.C. jail and speaking with inmates arrested in the U.S. Capitol insurrection case. A week ago, a federal judge raised questions about the treatment of those Jan. 6 inmates at the jail after revelations one of the defendants had a broken hand that was allegedly improperly cared for. [Continue Reading]

WaPo: **Former Chicago college student convicted of terrorism charge,** Unattributed, October 18, 2021, 8:37 PM

A former Chicago college student was convicted Monday of attempting to provide material support to the Islamic State group. Thomas Osadzinski, 22, designed a computer code to help the Islamic State bypass programs designed to block the group's propaganda, prosecutors said. The former DePaul University student, who was born in a Chicago suburb, was living in the city when he was arrested in 2019 during an FBI sting. He faces up to 20 years in prison. [Continue Reading] **See also:** WBBM-CBS (Chicago, IL)

ABC: **Sinclair Broadcast Group hit with ransomware attack,** Luke Barr, October 18, 2021, 5:34 PM
Sinclair Broadcast Group, which owns almost 300 stations across the country and provides local news services, was the victim of a ransomware attack over the weekend, the company announced in a Securities and Exchange Commission filing on Monday. "On October 16, 2021, the Company identified and began to investigate and take steps to contain a potential security incident. On October 17, 2021, the Company identified that certain servers and workstations in its environment were encrypted with ransomware, and that certain office and operational networks were disrupted," the filing says. [Continue Reading] **See also:** The Hill

Fox: **Illinois man pleads guilty to funding Brooklyn residents' trips to Syria to join ISIS, al-Nusra Front,** Bradford Betz, October 18, 2021, 5:27 PM
An Uzbekistan-born Illinois man pleaded guilty Thursday to helping fund overseas trips for people joining the Islamic State and al-Nusra Front (ANF). Dilshod Khusanov, 36, of Chicago, faces a maximum penalty of 11 years in prison. Per his plea agreement, Khusanov agreed to be removed from the U.S. after completing his sentence, the Justice Department said. [Continue Reading]

The Hill: **Agencies say agriculture groups being targeted by BlackMatter ransomware**, Maggie Miller, October 18, 2021, 5:03 PM
A trio of federal agencies on Monday sounded the alarm about critical infrastructure groups, particularly agricultural organizations, being targeted by a prolific ransomware group. The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) put out a joint advisory warning of targeting by "BlackMatter ransomware," connecting the group to previous attacks this year. [Continue Reading]

Yahoo News: **Civil liberties groups push Biden administration to drop case against Assange,** Zach Dorfman and Michael Isikoff, October 18, 2021, 10:30 AM
A group of civil liberties and human rights organizations are making an urgent appeal to Attorney General Merrick Garland to drop the criminal prosecution of Julian Assange in light of what it called a "shocking" Yahoo News story recounting how in 2017 senior CIA officials plotted to kidnap the WikiLeaks founder and even discussed possibly assassinating him. The groups have previously asked Garland to abandon the Assange case on the grounds that his prosecution for publishing classified documents would be a threat to First Amendment press freedoms. [Continue Reading]

NBC News Now: **[VIDEO] Crackdown on Chinese spying at American universities backfires,** Ken Dilanian, October 19, 2021, 6:00 AM
A Justice Department effort to root out Chinese espionage at universities has run into controversy. A series of criminal cases brought by prosecutors against professors and researchers as part of the "China Initiative" have fallen apart. Critics are accusing the government of overreaching and Asian-American groups are concerned the FBI has engaged in racial profiling. [Watch]

JAN. 6 COMMITTEE

AP: **Trump files lawsuit to keep Jan. 6 documents from Congress,** Jill Colvin, Colleen Long And Zeke Miller, October 18, 2021, 11:30 PM
Former President Donald Trump on Monday sought to block the release of documents related to the

Jan. 6 Capitol insurrection to a House committee investigating the attack, challenging President Joe Biden's initial decision to waive executive privilege. In a federal lawsuit, Trump said the committee's August request was "almost limitless in scope," and sought many records that weren't connected to the siege. He called it a "vexatious, illegal fishing expedition" that was "untethered from any legitimate legislative purpose," according to the papers filed in federal court in the District of Columbia. [Continue Reading] **See also:** ABC, Bloomberg, Business Insider, BuzzFeed, CBS, CNN, Courthouse News, The Hill, NBC, NBC-2, NPR, NYT, Politico, Reuters, USA Today, Washington Examiner, WSJ

Reuters: **U.S. House committee rejects Bannon 'privilege' argument in Jan. 6 probe**, Patricia Zengerle and Jan Wolfe, October 18, 2021, 8:21 PM
The U.S. congressional committee investigating the deadly Jan. 6 attack on the Capitol said on Monday that it rejected Steve Bannon's arguments for failing to cooperate with the probe, as the panel pursues a contempt of Congress charge against the long-time adviser to former President Donald Trump. [Continue Reading] **See also:** CNN, The Hill, WaPo, Yahoo News

CRIMINAL LAW

Reuters: **Russian businessman funded ex-Giuliani associates' account, court records show**, Lu Cohen, October 18, 2021, 6:34 PM
A Russian businessman funded an account used by two ex-associates of Rudy Giuliani to donate to U.S. political campaigns, according to documents shown in court on Monday. Prosecutors presented the financial records to a Manhattan federal court jury in the second week of the trial of one of the former associates, Lev Parnas, on charges of violating campaign finance laws. [Continue Reading] **See also:** Politico

WaPo: **Navy contractor voluntarily returns to U.S. to face bribery charge,** Craig Whitlock and Spencer S. Hsu , October 18, 2021, 7:24 PM
A defense contractor accused of slipping envelopes stuffed with more than $30,000 in cash to a U.S. Navy official appeared Monday in federal court in Washington and pleaded not guilty to a charge of bribery. Frank Rafaraci, 69, the chief executive of Multinational Logistics Services (MLS), a major U.S. Navy contractor, was arrested Sept. 27 on the Mediterranean island of Malta in an operation jointly planned by U.S. and Maltese authorities. He voluntarily returned to the United States on Monday to face the charge against him and was released on $5 million bond. [Continue Reading]

Bloomberg: **Maduro Ally in Court on Laundering Charges Amid U.S.-Venezuela Tensions**, Fabiola Zerpa and Nicolle Yapur, October 18, 2021, 5:43 PM
Colombian businessman Alex Saab, who's charged in the U.S. with money laundering stemming from allegedly brokering crooked deals for Venezuela's government while stealing hundreds of millions of dollars, is a flight risk who should be jailed until trial, prosecutors said. Making his first appearance in a U.S. court since losing a drawn-out extradition battle, Saab, 49, with shoulder-length hair and wearing an orange prisoner's jumpsuit, appeared on a video feed Monday from a jail cell. His lawyer asked for time to hold a pre-trial detention hearing. [Continue Reading] **See also:** Law360

Houston Chronicle: **Houston doctor who prescribed more than 1.3 million doses of opioids faces lengthy prison term**, Gabrielle Banks, October 18, 2021, 7:14 PM
A federal jury found a Houston physician guilty on Monday of prescribing more than 1.3 million doses of opioids through a strip mall clinic on Gessner in Spring Branch, according to a Justice Department news release. On a busy day, the doctor sometime doled out more than 90 unlawful prescriptions to "patients," prosecutors said. Dr. Parvez Anjum Qureshi, 56, a geriatric and family medicine specialist from Houston, was convicted of unlawfully prescribing controlled substances between 2014 and 2016 to patients at Spring Shadows Medical Clinic of Houston. [Continue Reading]

Pittsburgh Tribune-Review: **Hacker who sold UPMC employee data on the dark web sentenced to prison,** Michael DiVittorio, October 18, 2021, 6:31 PM
A Michigan man was sentenced Monday to seven years in prison for hacking into UPMC databases and stealing data of more than 65,000 employees and selling it on the dark web in 2014. U.S. District Chief Judge Mark Hornak imposed the maximum sentences against Justin Sean Johnson, 30, for the crimes of conspiracy to defraud the country and aggravated identity theft. [Continue Reading]

CIVIL RIGHTS

Reuters: **University of North Carolina defeats challenge to race-based admissions policies**, Nate Raymond, October 18, 2021, 7:21 PM
A federal judge on Monday ruled the University of North Carolina at Chapel Hill did not discriminate against white and Asian American applicants in a closely watched case challenging the consideration of race in undergraduate student admissions. The ruling by U.S. District Judge Loretta Biggs in Winston-Salem came in a lawsuit by Students for Fair Admissions, a group founded by conservative anti-affirmative action activist Edward Blum that is pursuing a similar case against Harvard University. [Continue Reading] **See also:** CNN, NYT, WSJ

AP: **Jury selection begins in trial over Ahmaud Arbery's death**, Russ Bynum, October 18, 2021, 4:00 PM
As jury selection got slowly underway Monday in the trial of three white men charged with fatally shooting Ahmaud Arbery as he was running in their Georgia neighborhood, potential jurors said they came in with negative feelings about the case and worried about the personal consequences of serving on the jury. [Continue Reading] **See also:** Courthouse News, Politico, Reuters, WSJ

The Hill: **Civil rights groups sue in Texas over redrawn House district maps**, Joseph Choi, October 18, 2021, 8:26 PM
Texas civil rights groups on Monday filed a federal lawsuit over the state's newly redrawn U.S. House districts, alleging that they were designed to dilute the voting power of minorities. The suit, filed my multiple minority rights groups, accuses Republican lawmakers of diluting the political power of Latinos in particular, according to The Associated Press. [Continue Reading]

Lexington Herald Leader: **U.S. Attorney settles with Lexington's Sayre School in disability discrimination case,** Valarie Honeycutt Spears, October 18, 2021, 4:41 PM
The U.S. Attorney's Office on Monday announced a settlement with Lexington's private Sayre School that ensures individuals with disabilities have equal access to the school's facilities. The settlement agreement resolves a disability discrimination complaint initiated in 2016 by the government under the Americans with Disabilities Act. A complaint was filed alleging there were physical access barriers at Sayre's Lower School. [Continue Reading]

IMMIGRATION & BORDER SECURITY

WaPo: **Biden's pick to lead Customs and Border Protection faces Senate confirmation hearing**, Nick Miroff, October 19, 2021, 5:00 AM
President Biden's nominee to lead U.S. Customs and Border Protection will face questions from the Senate Finance Committee on Tuesday morning in a long-delayed confirmation hearing that comes amid deepening Republican and Democratic frustrations with White House immigration policy. Biden's pick, Tucson Police Chief Chris Magnus, would take over the nation's largest law enforcement agency at a time when border agents are facing crisis-level workloads and their mission has become increasingly politicized. [Continue Reading]

CNN: **New DHS intelligence effort aims to better monitor and prepare for migrant surges**, Geneva

Sands and Priscilla Alvarez, October 18, 2021, 2:00 PM
The Department of Homeland Security is setting up a new intelligence gathering and law enforcement unit to monitor the movement of migrants journeying to the US southern border after being caught by surprise last month when thousands of people arrived in Del Rio, Texas. The initiative is aimed at improving the department's operational ability to prepare for potential migrant surges, according to DHS. The cell, first reported by NBC, is expected to be operational by the end of the month, according to a Homeland Security official. [Continue Reading]

Law360: **Feds, Migrants Say Texas Is Tardy To Title 42 Appeal,** Grace Dixon, October 18, 2021, 7:33 PM
The federal government and a class of migrant families excoriated Texas' 11th-hour attempts to intervene in litigation challenging the federal government's use of a public health law to expel migrant families, telling the D. C. Circuit that the motion comes months too late. The state of Texas had sought to weigh in on the federal government's use of Title 42 to turn away migrants at the border amid the COVID-19 pandemic, citing its interest in protecting residents from unvaccinated noncitizens traveling from Mexico. [Continue Reading]

ANTITRUST

Reuters: **Former Security Services Executives Plead Guilty to Rigging Bids for U.S. Security Contracts**, Kanishka Singh, October 18, 2021, 12:53 PM
Two former employees of security company G4S Secure Solutions NV pleaded guilty to criminal antitrust charges stemming from their involvement in a conspiracy to rig bids, fix prices, and allocate customers for defense-related security services contracts, the U.S. Justice Department said on Monday. "Bart Verbeeck, former director of sales, and Robby Van Mele, former director of operations, admitted that they, with their co-conspirators at competing firms, colluded to allocate security services contracts and to fix the prices at which the firms bid for contracts", the DOJ said in a statement. [Continue Reading]
See also: Law360

Law360: **Kroger, Others Settle Chicken Price-Fixing Suit Against Tyson**, Melissa Angell, October 18, 2021, 10:17 PM
Tyson Foods Inc. on Monday reached an agreement with Kroger, a handful of grocers and other food companies to settle part of a massive price-fixing litigation accusing multiple major chicken producers of conspiring with one another to fix the price of broiler chicken. [Continue Reading]

ENVIRONMENT

Newsweek: **New York Man Posing as Rescue Organization Charged With Trafficking Exotic African Cats,** Toria Barnhart, October 18, 2021, 8:25 PM
A New York man will spend 18 months in prison for trafficking exotic African cats after he posed as a big cat rescue organization. Christopher Casacci, 39, of Amherst, was sentenced in the Western District of New York for violating Lacey Act and the Animal Welfare Act by trafficking African wild cats, according to the Department of Justice (DOJ). The man, who was previously indicted in January 2020, operated the website ExoticCubs.com where he advertised, imported and sold African cats. [Continue Reading]
See also: WENY-ABC/CBS/CW (Elmira, NY), WETM-NBC (Elmira, NY), WGRZ-NBC (Buffalo, NY), WIVB-CBS (Buffalo, NY)

FEDERAL LAW ENFORCEMENT AGENCIES

Reuters: **FBI involved in effort to recover U.S. missionaries kidnapped in Haiti - source**, Unattributed, October 18, 2021, 2:02 PM
The FBI will assist in the investigation and efforts to locate and free a group of U.S. Christian

missionaries who have been kidnapped and are being held by a criminal gang in Haiti, a U.S. law enforcement official told Reuters on Monday. [Continue Reading] **See also:** Al Jazeera, WABC-ABC (New York, NY), WCAU-NBC (Philadelphia, PA), WOIO-CBS (Cleveland, OH), WSJ

CNN: **There was a 7.2% jump in assaults on law enforcement officers in 2020,** FBI says, Josh Campbell, October 19, 2021, 1:16 AM
More than 60,000 law enforcement officers were assaulted in the line of duty last year, up 7.2% from 2019, according to a report released Monday by the FBI. Around 30% of the officers sustained injuries, the FBI said. In a separate report in May, the agency reported that 93 officers were killed in the line of duty last year, including 46 deaths due to felonious acts. That number compared with 48 officers killed in felonious acts in 2019 and 41 killed in accidents. [Continue Reading] **See also:** Boston Herald, KTTN (Trenton, MO)

The Hill: **US Marshals allegedly ambushed Brian Laundrie lookalike on Appalachian Trail,** Sarakshi Rai, October 18, 2021, 1:46 PM
U.S. Marshals allegedly ambushed an innocent man who they mistakenly believed to be fugitive Brian Laundrie, wanted in connection with the Gabby Petito homicide case, The New Yorker reported Saturday. Severin Beckwith and his partner Anna Brettmann, both from Ithaca, N.Y., were woken up at their North Carolina hotel with a knock on the door and U.S. Marshals bursting in with guns drawn while on a hiking trip from Georgia to Virginia along the Appalachian Trail. [Continue Reading] **See also:** Deseret News (Salt Lake City, UT), KUSA-NBC (Denver, CO), Insider, Newsweek, Patch (Sarasota, FL)

US SUPREME COURT

WSJ: **[EDITORIAL] Progressive Court-Packing Meltdown**, Editorial Board, October 18, 2021, 6:46 PM
An early sign that President Biden would follow rather than lead his party was his refusal to repudiate "court-packing" in the 2020 campaign. As President he still had a chance to dismiss the idea as an exercise in constitutional arson. Instead, he appointed a commission to study packing the Supreme Court. [Continue Reading]

NYT: **In Two Rulings, Supreme Court Bolsters Legal Shield for Police**, Adam Liptak, October 18, 2021, 4:00 PM
In two unsigned decisions without noted dissents, the Supreme Court on Monday ruled in favor of police officers accused of using excessive force. The rulings were a signal that the court continues to support the doctrine of qualified immunity, which can shield police misconduct from lawsuits seeking damages. The doctrine has been the subject of criticism across the ideological spectrum, and it became a flash point in the nationwide protests last year over police brutality, with activists and lawmakers calling for its reconsideration. [Continue Reading] **See also:** CNN, Courthouse News, NBC, WaPo, WSJ

The Hill: **DOJ says Guantanamo detainee can testify about his CIA torture,** Joseph Choi, October 18, 2021, 7:49 PM
The Department of Justice (DOJ) said in a letter to the Supreme Court last week that a Guantanamo Bay detainee will be allowed to testify about the alleged torture he experienced. Acting Solicitor General Brian Fletcher wrote in a letter to the Supreme Court on Friday that Abu Zubaydah would be permitted to tell authorities in Poland about his alleged torture. [Continue Reading]

Politico: **Pence group backs coach at Supreme Court in school prayer case,** Josh Gerstein, October 18, 2021, 2:56 PM
A religious freedom group headed by former Vice President Mike Pence is urging the Supreme Court to take up a case involving a football coach who was fired for praying on the field at the end of games. The

Pence group — Advancing American Freedom — was among about 70 organizations and individuals who joined in an amicus brief filed Monday asking the justices to hear the case of Joseph Kennedy, who was dismissed in 2015 as the coach at Bremerton High School in Washington state. [Continue Reading]

SCOTUSblog: **Court adds two cases on Native American law and issues two opinions granting police officers qualified immunity**, Amy Owe, October 18, 2021, 12:39 PM
The Supreme Court on Monday morning added two new cases, both involving Native Americans, to its docket for this term. The justices also issued two unsigned decisions holding, without oral argument, that police officers are entitled to qualified immunity from lawsuits accusing them of using excessive force. The justices, however, did not act on several of the high-profile petitions that they considered at their private conference last week. [Continue Reading]

ADMINISTRATION

AP: **EPA unveils strategy to regulate toxic 'forever chemicals',** Matthew Daly, October 18, 2021, 3:49 PM
The Biden administration said Monday it is launching a broad strategy to regulate toxic industrial compounds associated with serious health conditions that are used in products ranging from cookware to carpets and firefighting foams. Michael Regan, the head of the Environmental Protection Agency, said his agency is taking a series of actions to limit pollution from a cluster of long-lasting chemicals known as PFAS that are increasingly turning up in public drinking water systems, private wells and even food. [Continue Reading] **See also:** Courthouse News, Law360, WaPo

CONGRESS

The Hill: **Senate Democrats ask for details on threats against election workers,** Jordain Carney, October 18, 2021, 2:20 PM
Senate Democrats are pushing the Department of Justice (DOJ) for details on threats against election workers and any related probes. Senate Rules Committee Chairwoman Amy Klobuchar (D-Minn.), Senate Judiciary Committee Chairman Dick Durbin (D-Ill.) and 19 other Democratic senators sent a letter to the Justice Department on Monday asking for updates from the Election Threats Task Force, which the DOJ formed earlier this year to combat threats against election workers. [Continue Reading]

NETWORK EVENING NEWS LINEUP: OCTOBER 18, 2021

- Colin Powell, the retired four-star general who became the country's first Black secretary of state and chairman of the Joint Chiefs of Staff, died Monday due to complications from COVID-19, his family said. [ABC, CBS, NBC]
- The FBI and US State Department have joined efforts to free 17 missionaries who were kidnapped in Haiti. Violence and crime have spun out of control there since Haiti's president was assassinated in July. [ABC, CBS, NBC]
- Jury selection began Monday in Georgia in the trial of three white men charged in the death of Ahmaud Arbery, who was fatally shot as he was running in their neighborhood in February 2020. The three men, father and son Gregory and Travis McMichael and their neighbor William "Roddie" Bryan, are charged with murder and aggravated assault. [ABC, CBS, NBC]
- Former President Donald Trump on Monday sought to block the release of documents related to the Jan. 6 Capitol insurrection to a House committee investigating the attack, challenging President Joe Biden's initial decision to waive executive privilege. [CBS, NBC]
- After the mayor's vaccine mandate went into effect over the weekend in Chicago, termination is on the line for possibly thousands in the city's police force. Similar mandates are taking effect in cities across the US. [ABC, NBC]
- Some parents are pushing back over a California order requiring all students to get vaccinated

against COVID-19 once they are eligible and the FDA gives full approval. [CBS]

- Law enforcement is still searching for the gunman who opened fire on three deputies in Houston. One, who had recently become a father, was killed. [CBS]
- China said Monday its launch of a new spacecraft was merely a test to see whether the vehicle could be reused. The launch involved a spacecraft rather than a missile and was of “great significance for reducing the use-cost of spacecraft and could provide a convenient and affordable way to make a round trip for mankind’s peaceful use of space,” Foreign Ministry spokesperson Zhao Lijian said. [ABC]
- Retired British spy Christopher Steele is stepping out of the shadows to discuss his so-called "Steele dossier" for the first time publicly, describing his efforts as apolitical and defending his decision to include the most explosive and criticized claims about Donald Trump contained in his controversial 2016 report. [ABC]

From: Coley, Anthony D. (PAO)
Subject: Abbreviated AM Clips
To: Klapper, Matthew B. (OAG)
Cc: Iverson, Dena (PAO); Heinzelman, Kate (OAG); Seidman, Ricki (OASG); Fletcher, Brian H. (OAG); Goodlander, Margaret V. (OAG); Matthews-Johnson, Tamarra D. (OAG); Visser, Tim (OAG)
Sent: July 27, 2021 7:36 AM (UTC-04:00)

US DEPARTMENT OF JUSTICE NEWS

WSJ: **Aon-Willis Deal Faced High Hurdle With Garland Heading Justice Department,** John D. McKinnon and Aruna Viswanatha, July 26, 2021, 4:15 PM
The decision by insurance brokers Aon PLC and Willis Towers Watson PLC to scuttle their $30 billion merger underscores the hard line the Biden administration is forming on antitrust and competition issues. The two companies abandoned their deal Monday, citing the futility of going forward after the Justice Department filed suit to block it last month. [Continue Reading] **See also:** CNN, WaPo, WSJ-1

CNN: **Federal law doesn't prohibit Covid-19 vaccine requirements, Justice Department says,** Evan Perez and Tierney Sneed, July 26, 2021, 5:54 PM
Justice Department lawyers have determined that federal law doesn't prohibit public agencies and private businesses from requiring Covid-19 vaccines -- even if the vaccines have only emergency use authorization, according to an opinion posted online Monday. The opinion from the department's Office of Legal Counsel paves the way for more federal agencies and businesses to require vaccinations. The Department of Veterans Affairs announced on Monday that it will require many of its front-line health care workers to be vaccinated against Covid. The VA is the first in the federal government to require shots among its workers. [Continue Reading] **See also:** Politico

US ATTORNEYS

AP: **8 US Attorney Picks by Biden Would Include Historic Firsts,** Eric Tucker, July 26, 2021, 2:35 PM
President Joe Biden is nominating eight new leaders for U.S. attorney positions across the country, including in the office overseeing the prosecutions of hundreds of defendants charged in the Jan. 6 insurrection at the Capitol. The nominees announced by the White House on Monday come as the Justice Department is continuing to round out its leadership team under Attorney General Merrick Garland, who traveled to Chicago last week to announce an initiative to crack down on gun trafficking corridors. [Continue Reading] **See also:** WSJ

NYT: **A veteran prosecutor was tapped to lead the U.S. Attorney's Office in Washington.,** Katie Benner, July 26, 2021, 5:50 PM
The White House on Monday nominated a former federal prosecutor to lead the U.S. Attorney's office in Washington, overseeing high-profile investigations including the prosecutions of hundreds of Trump supporters charged in the Jan. 6 attack on the Capitol. The nominee, Matt Graves, a longtime veteran of the office, led its fraud and public corruption unit before becoming a partner at DLA Piper, a prominent white-shoe law firm. [Continue Reading]

Baltimore Sun: **Biden nominates Erek Barron to be U.S. Attorney for Maryland, first Democrat nominated in 20 years,** Justin Fenton, July 26, 2021, 1:45 PM
President Biden has nominated Prince George's County Del. Erek Barron to become the next U.S. Attorney for Maryland — who would be the first Black person to hold the post, and the first Democrat in 20 years, if confirmed. Barron, 47, a defense attorney, has been a member of the House of Delegates since 2015. Before that he worked stints as a federal prosecutor and as an assistant state's attorney in Prince George's and Baltimore. [Continue Reading] **See also:** WBAL-NBC (Baltimore, MD), WJZ-CBS

(Baltimore, MD), WMAR-ABC (Baltimore, MD)

Boston Globe: **Biden nominates Rachael Rollins as US Attorney for Massachusetts,** Andrea Estes and Jim Puzzanghera, July 26, 2021, 10:06 AM
President Biden nominated Suffolk County District Attorney Rachael Rollins to be US Attorney from Massachusetts on Monday. If confirmed by the Senate, Rollins, a criminal justice reformer, would be the first Black woman to hold the role in the state, overseeing an office of more than 200 federal prosecutors. [Continue Reading] **See also:** Boston Globe-2, Law 360, WBTS-NBC (Boston, MA), WCVB-ABC (Boston, MA)

Indianapolis Star: **President Biden nominates Indiana's first Black US Attorneys,** Serena Puang, July 26, 2021, 11:46 (EDT)
President Joe Biden nominated Clifford D. Johnson and Zachary A. Myers for United States Attorney in the Northern and Southern districts, respectively, of Indiana today. According to a White House spokesperson, both nominees would be the first Black U.S. Attorneys for their respective districts if confirmed by the U.S. Senate. [Continue Reading]

WGRZ-NBC (Buffalo, NY): **President Biden nominates Trini Ross to be next US Attorney for the Western District of New York,** Unattributed, July 26, 2021, 12:36 PM
President Joseph Biden on Monday announced his nominee to become the next U.S. Attorney for the Western District of New York. If confirmed by Congress, Trini E. Ross, a graduate of SUNY Fredonia and UB Law School, will become the first African-American female to serve in the position. [Continue Reading] **See also:** WIVB-CBS (Buffalo, NY)

Law360: **Boston Defense Attys Welcome Friendlier DOJ Under Rollins**, Unattributed, July 26, 2021, 9:16 PM
Local Boston defense attorneys hailed the Biden administration's selection of Suffolk County District Attorney Rachael Rollins as Massachusetts' next U.S. attorney, saying the progressive prosecutor has the potential to curb excessive white collar sentences and bring about "seismic change" to the high-profile office. [Continue Reading] **See also**: WYCN-NBC (Boston, MA)

NATIONAL SECURITY

USA Today: **Former Trump aide Thomas Barrack pleads not guilty to illegal lobbying charges,** Kevin Johnson, July 26, 2021, 2:43 PM
Thomas Barrack, who chaired former President Donald Trump's inaugural committee, and a co-defendant pleaded not guilty Monday to illegal lobbying charges related to their alleged attempts to advance the interests of the United Arab Emirates with the Trump campaign and the former president's administration. Barrack, 74, and Matthew Grimes, 27, entered their pleas in a Brooklyn, N.Y., federal court following their arrests last week. [Continue Reading] **See also:** CBS, CNN, Politico, WaPo

LAT: **After feds drop charges against Chinese scholars, new concerns about racial profiling,** Del Quentin Wilber, Leila Miller, and Teresa Watanabe, July 26, 2021, 11:01 PM
When the Trump administration in 2018 unveiled a sweeping crackdown on economic espionage by the Chinese government, advocacy groups and academics raised concerns the effort could result in racial profiling and have a chilling effect on collaborations. Then last week, federal prosecutors abruptly dropped charges against five Chinese researchers at U.S. universities accused of visa fraud, fueling fresh doubts about the "China Initiative" and bringing new calls for the Justice Department to end or revamp it. [Continue Reading]

CNN: **Biden to address intelligence community for first time as President**, Katie Bo Williams, July

27, 2021, 5:00 AM
Six months into Joe Biden's presidency, the intelligence community still can't quite escape politics. Biden will make his first formal remarks to staff at the Office of the Director of National Intelligence on Tuesday, an address that comes at a moment of quiet but profound change for a workforce that was buffeted by the fierce political winds of the Trump era. [Continue Reading]

NPR: **A Lawsuit Against Jan. 6 Rally Speakers Forces DOJ To Consider Who's Legally Immune,** Carrie Johnson, July 26, 2021, 4:03 PM
A lawsuit against the men who spoke at a rally before the Capitol riot on Jan. 6 is putting the Justice Department in a tricky position. The department is considering whether those federal officials acted within the scope of their jobs that day, which would trigger a form of legal immunity. Government watchdogs said the case has serious implications for who's held accountable for violence that delayed the election certification and contributed to the deaths of five people. [Continue Reading] **See also:** The Birmingham News (Birmingham, AL)

WaPo: **[OPINION] Merrick Garland, don't politicize the pursuit of justice,** Jennifer Rubin, July 26, 2021, 7:45 AM
On Tuesday, the Justice Department and the House of Representatives will file briefs explaining to a federal court whether each believes that Rep. Mo Brooks (R-Ala.) was acting within the scope of his employment when he allegedly incited the violent attack on the Capitol and sought to subvert the peaceful transfer of power on Jan. 6. This sounds absurd, but in effect Brooks is asking the Justice Department to certify that he was acting in the scope of his duties when he tried to overthrow the government. [Continue Reading]

JAN. 6 HOUSE COMMITTEE

WaPo: **[OPINION] We have started investigating the Jan. 6 attack on the Capitol. Nothing will be off-limits,** Bennie G. Thompson, July 26, 2021, 4:15 PM
On Jan. 6, a violent mob attacked the citadel of our democracy — the U.S. Capitol — in an attempt to prevent Congress from doing its constitutional duty to certify the results of the 2020 presidential election. On Tuesday, the bipartisan Select Committee on the January 6th Attack on the United States Capitol begins its work investigating the facts, circumstances and causes of this assault on our democracy. [Continue Reading]

WaPo: **[EDITORIAL] We have questions about Jan. 6. The new House committee can answer them**, Editorial Board, July 26, 2021, 5:23 PM
The House select committee investigating the Jan. 6 Capitol insurrection begins work Tuesday, hearing from police officers who confronted the deadly chaos. Reminding Americans that the Jan. 6 riot was a horrific attack on democracy — in contrast to the narrative some Republicans have told of a "loving crowd" filled with people behaving like average Washington tourists — is an essential part of the committee's work. But, also in contrast to Republican claims, there is much for the select committee to uncover. [Continue Reading] **See also:** CNN, NYT

Politico: **Democrats prep a somber yet TV-ready first hearing in Jan. 6 probe,** Nicholas Wu, Heather Caygle and Olivia Beavers, July 27, 2021, 4:30 AM
Democrats want Americans glued to their TVs Tuesday for the first hearing of the Jan. 6 select committee. They also don't want a circus. More than six months since the deadly siege of the Capitol, the select panel's first meeting is designed as a somber yet camera-ready event to elicit fading memories of that day's horrifying events — not to mention counter a GOP wave of revisionist history that threatens to muddy the waters. [Continue Reading]

Forbes: **House GOP's Top Capitol Riot Downplayers Plan DOJ Stunt To Counter First Jan. 6 Panel Hearing,** Andrew Solender, July26, 2021, 4:54 PM
Four House Republicans who have repeatedly downplayed the severity of the Jan. 6 attack on the U.S. Capitol will hold a press conference outside the Department of Justice on Tuesday, part of a broader GOP effort to distract from the Jan. 6 select committee's first hearing. Reps. Matt Gaetz (R-Fla.), Louie Gohmert (R-Texas), Paul Gosar (R-Ariz.) and Marjorie Taylor Greene (R-Ga.) will be "demanding answers on the treatment of January 6th prisoners" outside the DOJ's D.C. office, according to Gohmert's office. [Continue Reading] **See also:** The Hill

CRIMINAL LAW

Bloomberg: **Cuomo Takes Victory Lap After DOJ Drops N.Y. Nursing Home Probe,** Emma Kinery, July26, 2021, 3:33 PM
New York Governor Andrew Cuomo said the U.S. Department of Justice's decision to drop an investigation into whether he mishandled Covid-19 outbreaks in nursing homes vindicated his administration and that he is "eager" for the results of other probes into his alleged misconduct. The Justice Department on Friday said it wouldn't investigate New York's handling of coronavirus in its nursing homes, along with identical investigations into New Jersey, Pennsylvania and Michigan. Cuomo said the decision showed the probe, initiated under the Trump administration, was politically motivated. [Continue Reading] **See also:** NY Post

CIVIL RIGHTS

CNN: **DOJ defends 2 Texas teens in fight with school district over long locs,** Christina Carrega, July 26, 2021, 4:58 PM
The Justice Department has stepped into a legal dispute on behalf of two Texas male students who say their school district discriminated against them when they were not allowed to attend classes because they refused to cut the length of their hair that they wore in locs. "The United States has a significant interest in ensuring that all students can participate in an educational environment free of unlawful discrimination and in the proper application of the Equal Protection Clause, Title IX, and Title VI," according to the statement of interest that was filed on Friday. [Continue Reading]

KMBC-ABC (Kansas City, MO): **Local civil rights leaders want Department of Justice to investigate the Kansas City Police Department,** Micheal Mahoney, July26, 2021, 5:09 PM
Some Kansas City civil rights leaders want the U.S. Department of Justice to investigate the Kansas City Police Department from top to bottom. The group says they want an investigation like the DOJ's investigation of the Ferguson Police Department in 2015. That report found patterns of racial bias in the Ferguson, Missouri, police department and at the municipal jail and court. [Continue Reading]

IMMIGRATION & BORDER SECURITY

NYT: **U.S. Can Expedite Removal of Migrant Families, Biden Administration Says**, Miriam Jordan, July 26, 2021, 11:00 PM
The Biden administration announced late Monday that it would begin swiftly removing migrant families that immigration officials determined did not qualify for asylum after an initial screening at the southwestern border. The policy, known as expedited removal, is a return to a measure that has been used by Democratic and Republican administrations to deter unauthorized immigration. Asylum officers interview families in a fast-tracked screening process to determine if they have a "credible fear of persecution." [Continue Reading]

NYT: **ICE detainees at Bergen County jail allege abuse, medical neglect**, Miriam Jordan, July 26, 2021, 3:00 PM
Alex Murillo leads a full life in the Mexican town of Rosarito, a 40-minute drive from the U.S. border near Tijuana. By day, he works at a call center, speaking in a cheerful, caring tone to retirees across the United States about their Medicare insurance. [...] Many veterans said they did not realize they could be deported until an officer from Immigration and Customs Enforcement showed up at the end of their prison sentence. Many feel wronged that, after serving their time, they face additional punishment. [Continue Reading] **See also:** NJ Spotlight

Fox: **ICE nabs more than 300 illegal immigrant sex offenders since June as part of national operation,** Adam Shaw, July 26, 2021, 5:47 PM
Hundreds of illegal alien sex offenders have been arrested by Immigration and Customs Enforcement (ICE) agents thanks to Operation Sex Offender Arrest and Removal (SOAR). On Monday, ICE officials announced that as of early June 4, 302 illegal aliens convicted of sex crimes have been arrested as part of Operation SOAR, which was launched by the agency in 2010. [Continue Reading]

Law360: **Garland Deals 4th Blow To Trump Policy In Asylum Order**, Unattributed, July 26, 2021, 8:07 PM
Attorney General Merrick Garland vacated a fourth ruling from his Trump-era predecessors on Monday, this time restoring immigration judges' discretion not to review stipulated material so they can focus on contested issues. [Continue Reading]

ANTITRUST

WSJ: **Judge Extends Deadline for FTC to Refile Facebook Antitrust Suit**, Ryan Tracy, July 26, 2021, 1:32 PM
The Federal Trade Commission has until Aug. 19 to file an amended version of its antitrust lawsuit against Facebook Inc. FB 0.72% after a judge granted the agency an extension. Judge James E. Boasberg of the U.S. District Court for the District of Columbia had previously set a July 29 deadline after saying the agency hadn't supported its claims that Facebook has monopoly power in personal social-networking services. His dismissal of the suit cited in part how the FTC calculated the company's market share. [Continue Reading]

Law360: **Perdue Inks Deal To Secure Exit From Chicken Price-Fix Suit**, Unattributed, July 26, 2021, 7:05 PM
Perdue Farms has quietly settled one of many suits accusing the poultry giant of participating in a cartel of rivals that colluded to keep the price of chicken high, according to documents filed in an Oklahoma federal court. [Continue Reading]

FEDERAL LAW ENFORCEMENT AGENCIES

Philly Voice: **Murder-for-hire plot thwarted in Southwest Philadelphia, prosecutors say**, Michael Tanenbaum, July 26, 2021, 7:00 PM
A Philadelphia man who allegedly attempted pay $5,000 to have a rival killed in a murder-for-hire plot was arrested last week by law enforcement officers, who believe multiple people may have been targets of violence had the plan not be foiled. The discovery of the alleged plot came as part of an ongoing state drug trafficking investigation, during which investigators became aware of communications initiated by 47-year-old Darnell Jackson, aka "Major Change." [Continue Reading] **See also:** KYW-CBS (Philadelphia, PA), Philadelphia Inquirer, WCAU-NBC (Philadelphia, PA), WHYY-FM (Philadelphia, PA), WPVI-ABC (Philadelphia, PA), WTXF-Fox (Philadelphia, PA)

New Jersey Advance Media: **FBI investigating cops' use of force while teen was being handcuffed, officials say,** Kevin Shea, July 26, 2021, 5:16 PM
The actions of Ewing police officers during the arrest of a Black teen suspect in 2018 are under investigation by the FBI, the town's mayor and police chief confirmed. Two officers appear to kick snow in the 16-year-old teen's face while he is face down on the ground being handcuffed, while a third apparently steps on his head, according to bodycam footage of the January 2018 incident, posted early Monday by the Trentonian newspaper. The paper was first to report last month that federal authorities were investigating. [Continue Reading]

Raleigh News & Observer: **Five Myrtle Beach area men among those charged in national cocaine-trafficking scheme**, Jenna Farhat, July 26, 2021, 3:04 PM
Six people have been arrested and charged federally, accused of working in a drug trafficking ring that operated between several South Carolina cities and New York City. U.S. Attorney for the district of South Carolina M. Rhett DeHart announced the charges Monday in a news release. The investigation from which the charges stemmed is led by the Drug Enforcement Administration (DEA), in collaboration with federal, state, and local law enforcement. [Continue Reading]

KRON (San Francisco, CA): **Oakland police, FBI announce new actions to prevent violent crime in Chinatown,** Dan Thorn, July 27, 2021, 1:51 AM
On Monday, Oakland's police chief, the FBI Special Agent, and other city leaders announced they'll be working together to stop violent crimes. There have been several attacks in Chinatown, many of those cases were caught on video, and some of those still have not been solved. Residents and business owners in the neighborhood have expressed their concern with the increase in crime but leaders say they're working to fight it. [Continue Reading] **See also:** KTVU-Fox (Oakland, CA)

WPIX-CW (New York, NY): **ATF working with NYPD to fight gun violence in NYC,** Jennifer Bisram, July26, 2021, 10:31 PM
While gun violence is up in NYC, so is enforcement and intelligence, according to the Bureau of Alcohol, Tobacco, Firearms and Explosives. Agents are focused on tracking down shooters who are connected to multiple crimes, something they've seen an increase of, ATF NY's Assistant Special Agent in Charge Daryl McCormick said. A new partnership between the federal agency and the NYPD was launched to get guns off city streets. [Continue Reading]

WDSU-NBC (New Orleans, LA): **Exclusive: Part 4: FBI begins Summer, Fall of anti-hate initiatives,** Mark Albert, July26, 2021, 5:21 PM
Emanating on a recent Friday night from the 121-year-old synagogue here was a sound hate could not silence. But the voices singing from the Torah during a Shabbat service under the stained glass windows and soaring sanctuary would have been snuffed out had Richard Holzer succeeded in his plan to "get that place off the map." [Continue Reading]

WNWO-NBC (Toledo, OH): **Toledo police to team up with ATF again to crack down on gun violence,** Unattributed, July26, 2021, 4:00 PM
In the wake of a violent weekend, the Toledo Police Department is bringing back Operation Clean Sweep for the second time this year. Friday through Sunday, officers will be collaborating with the Bureau of Alcohol, Tobacco, Firearms and Explosives to pursue federal charges against anyone illegally possessing firearms or using them in a violent crime or drug trafficking offense. [Continue Reading]

CONGRESS

Washington Times: **Grassley presses FBI to explain its monitoring of conservative women's**

group, Ryan Lovelace, July 26, 2021, 4:15 PM
Sen. Chuck Grassley is pressing the FBI to explain the reasoning for its newly revealed probe into the conservative group Concerned Women for America, The Washington Times has learned. The FBI's review of the pro-life women's organization has prompted an outcry from the group's leadership and others concerned about law enforcement and intelligence community surveillance of Americans. [Continue Reading]

The Hill: **Rand Paul sends official criminal referral on Anthony Fauci to DOJ,** Christian Spencer, July 26, 2021, 3:00 PM
Sen. Rand Paul (R-Ky.) made good on his threat to refer Anthony Fauci, chief medical adviser to President Biden and director of the U.S. National Institute of Allergy and Infectious Diseases, to the Justice Department for allegedly lying to Congress about funding gain-of-function research at the Wuhan Institute of Virology. [Continue Reading]

NETWORK EVENING NEWS LINEUP: JULY 26, 2021

- More than 50 health organizations are now calling for all health care workers to be required to get vaccinated, saying "the health and safety of US workers, families, communities, and the nation depends on it." Dr. Fauci warns that the US is moving in the wrong direction. In Jackson, Mississippi, 52-year-old William Ball is one of the 89% of hospitalized COVID patients who are not vaccinated. [ABC, CBS, NBC]
- A select congressional committee will launch its investigation into the deadly January 6 attack on the US Capitol on Tuesday. The inquiry is already coming under fire before it has even gavelled in. [ABC, CBS, NBC]
- President Biden announced that the US military combat mission in Iraq will be finished by the end of 2020. About 2,500 American troops remain in the country, but it's unclear how many will stay to train and assist Iraqi forces. [ABC, CBS, NBC]
- Tom Barrack, the close adviser to former President Trump, who also ran his inaugural committee, pleaded not guilty to federal charges of illegally lobbying for the UAE. He was released on a $250 million bond Friday - one of the largest criminal bails in history. [CBS]

From: Coley, Anthony D. (PAO)
Subject: Abbreviated AM Clips
To: Klapper, Matthew B. (OAG)
Cc: Iverson, Dena (PAO); Heinzelman, Kate (OAG); Seidman, Ricki (OASG)
Sent: June 8, 2021 7:53 AM (UTC-04:00)

US DEPARTMENT OF JUSTICE NEWS

AP: **US has recovered ransom payment made after pipeline hack,** Eric Tucker, June 7, 2021, 4:50 PM
The Justice Department has recovered the majority of a multimillion-dollar ransom payment to hackers after a cyberattack that caused the operator of the nation's largest fuel pipeline to halt its operations last month, officials said Monday. The operation to recover the cryptocurrency from the Russia-based hacker group is the first undertaken by a specialized ransomware task force created by the Biden administration Justice Department, and reflects what U.S. officials say is an increasingly aggressive approach to deal with a ransomware threat that in the last month has targeted critical industries around the world. [Continue Reading] **See also:** ABC, AFP, Bloomberg, CBS, Courthouse News, CNN, Financial Times, Guardian, KPIX-CBS (San Francisco, CA), LAT, Law360, NBC, NPR, NYT, NY Magazine, Reuters, USA Today, VOA, WaPo, Washington Examiner, Washington Times, WSJ

Reuters: **U.S. agents to start wearing body cameras when serving warrants,** Unattributed, June 7, 2021, 9:56 PM
U.S. law-enforcement agents will be required to wear body cameras when serving search and arrest warrants, the Justice Department said on Monday, adding a measure of accountability already required of many state and local police departments. Federal agents had previously been barred from wearing cameras, a policy that sometimes created tension during joint operations with state and local police. [Continue Reading] **See also:** CNN, LAT, Politico, WaPo, WSJ

AP: **Justice Dept. continues appeal on behalf of Trump in defamation case brought by sexual assault accuser,** Larry Neumeister, June 7, 2021, 11:53 PM
Donald Trump cannot be held personally liable for "crude" and "disrespectful" remarks he made while president about a woman who accused him of rape, Justice Department lawyers said Monday in arguing for him to be replaced by the United States as defendant in a defamation lawsuit. The lawyers told the 2nd U.S. Circuit Court of Appeals in Manhattan that responding to allegations of misconduct falls within activities that form part of any president's office. Trump was acting "within the scope of his office" in denying wrongdoing after White House reporters asked him about claims by columnist E. Jean Carroll in a June 2019 book that he attacked her in the mid-1990s at an upscale Manhattan department store, the lawyers from the Washington office of the Justice Department wrote. [Continue Reading] **See also:** BuzzFeed, CBS, TheHill, HuffPost, NBC, Newsweek, NYT, Politico, WaPo, WSJ

CNN: **Justice Department unveils two anti-gun violence proposals after another violent weekend,** Christina Carrega, June 7, 2021, 12:51 PM
Attorney General Merrick Garland unveiled Monday two proposals meant to help curb gun violence, an announcement that comes after another violent weekend. The Justice Department proposed to clarify the restrictions on stabilizing braces that transform a pistol into a short-barreled rifle and can "cause great damage and are more likely to be used to commit crimes." [Continue Reading]

WaPo: **[EDITORIAL] The Justice Department turns around on press freedom — but is it for good?,** Editorial Board, June 7, 2021, 7:11 PM
The Justice Department announced Saturday that it will no longer pursue legal orders demanding reporters' communications records, after a series of disclosures of investigators seeking and in some cases obtaining information relating to journalists at The Post, the New York Times and CNN. The new policy is better than the previous rules, which proved deficient in protecting journalism. But the Biden administration must do more to reassure the media — and the public that depends on reporters doing their jobs — that it will not interfere with

newsgathering. [Continue Reading]

CAPITOL RIOT PROSECUTIONS

WaPo: **Capitol Police had intelligence indicating an armed invasion weeks before Jan. 6 riot, Senate probe finds,** Karoun Demirjian, June 8, 2021, 5:00 AM
The U.S. Capitol Police had specific intelligence that supporters of former president Donald Trump planned to mount an armed invasion of the Capitol at least two weeks before the Jan. 6 riot, according to new findings in a bipartisan Senate investigation, but a series of omissions and miscommunications kept that information from reaching front-line officers targeted by the violence. A joint report, from the Senate Rules and Administration and the Homeland Security and Governmental Affairs committees. [Continue Reading] **See also:** Axios, Fox, WSJ

FEDERAL LAW ENFORCEMENT AGENCIES

AP: **Global Sting: FBI-Encrypted App Tricks Organized Crime,** Mike Corder And Nick Perry, June 8, 2021, 5:54 AM
A global sting involving an encrypted communications platform developed by the FBI has sparked raids and arrests around the world, delivering "an unprecedented blow" to crime gangs, law enforcement authorities said Tuesday. Operation Trojan Shield involved police swoops in 16 nations. More than 800 suspects were arrested and more than 32 tons of drugs — cocaine, cannabis, amphetamines and methamphetamines were seized along with 250 firearms, 55 luxury cars and more than $148 million in cash and cryptocurrencies. [Continue Reading] **See also:** Axios

NYT: **F.B.I. Investigates Cyber Attack That Targeted N.Y.C. Law Department,** Benjamin Weiser and Ashley Southall, June 7, 2021, 8:01 PM
An early clue that something was amiss with the computers at New York City's Law Department — the 1,000-lawyer agency that represents the city in court — emerged on Monday when a lawyer for the department wrote to a federal judge in Manhattan, asking for a short delay in filing court papers because of "connectivity" problems. "No one is currently able to log on to the Law Department's computer system," the lawyer, Katherine J. Weall, wrote. [Continue Reading]

KMSP-Fox (Minneapolis, MN): **Ramsey County Sheriff: Deputies will not serve on U.S. Marshal task force until body cameras allowed,** Hannah Flood, June 7, 2021, 7:00 PM
Ramsey County Sheriff's deputies will no longer participate with the U.S. Marshals Fugitive Task Force until local law enforcement will be allowed to wear body cameras when serving on the task force, according to Ramsey County Sheriff Bob Fletcher. "The United States Marshals office has been misleading in their public comments in the media," said Fletcher in a statement to FOX 9. " [Continue Reading]

NATIONAL SECURITY

WSJ: **Tennessee Scientist Is First to Go on Trial on Charges He Hid Work in China,** Aruna Viswanatha, June 7, 2021, 5:50 PM
Until last year at the University of Tennessee, Anming Hu studied, among other things, how to join certain metals together using materials that are more than 1,000 times smaller than the width of a human hair. He also ran a group developing similar nanoscale technologies at an institute in Beijing. Mr. Hu's research has a range of potential applications including fixing turbines and printing sophisticated electronic sensors. On Monday, prosecutors began presenting their case in court, alleging that Mr. Hu hid his China collaborations from the U.S. government while also receiving National Aeronautics and Space Administration grants for his work in Tennessee. [Continue Reading]

IMMIGRATION & BORDER SECURITY

AP: **Deported veteran sues to get naturalization interview in US,** Amy Taxin, June 7, 2021, 7:55 PM

Hector Ocegueda-Rivera wanted to head to an interview in Los Angeles with immigration officers so he could become a U.S. citizen — but since he was deported to Mexico, he couldn't get back in the country to do so. Now, the 53-year-old U.S. Marine Corps veteran who was deported after a conviction for driving under the influence is suing to demand the U.S. government let him in to attend the interview or send an immigration officer to the border to speak with him so he can meet the requirements of becoming an American. [Continue Reading]

ABC: **Biden's task force finds more than 3,900 children separated from families at border under Trump,** Mike Levine and Luke Barr, June 07, 2021, 5:06 PM
The Biden administration has determined that more than 3,900 children were separated from their families along the Southwest border after the Trump administration launched its controversial "zero-tolerance policy," and -- while several hundred children were returned to their home countries -- fewer than 60 families are now in the process of being reunited, sources familiar with a new report from the Biden team told ABC News. The report has yet to be released publicly, but its findings mark an official assessment from the Department of Homeland Security and other federal agencies of how many children were actually impacted when the Trump administration decided to take what many considered drastic steps to fight illegal immigration. [Continue Reading]

US SUPREME COURT

Reuters: **U.S. Supreme Court rebuffs challenge to all-male military draft sign-up**, Lawrence Hurley, June 7, 2021, 9:40 PM
The U.S. Supreme Court on Monday declined to hear a challenge by a men's rights group to the national requirement that men, but not women, register for the military draft at age 18, focusing on whether the policy violates the U.S. Constitution's guarantee that laws apply equally to everyone. [Continue Reading]

WSJ: **Supreme Court to Consider State-Secrets Case on Government Surveillance,** Brent Kendall, June 7, 2021, 3:49 PM
The Supreme Court on Monday agreed to consider a U.S. government appeal that seeks dismissal of a case involving allegations of improper surveillance of Muslims, on the grounds that further litigation risks disclosing state secrets. The high court separately declined to consider a sex-discrimination challenge to the longstanding requirement that only men register for the military draft when they turn 18 years of age. [Continue Reading]

WSJ: **Supreme Court Says Protected Noncitizens Who Entered U.S. Unlawfully Can't Get Green Cards,** Jess Bravin, June 7, 2021, 1:37 PM
The Supreme Court said Monday that noncitizens who entered the U.S. unlawfully can't obtain permanent residency even if the government has permitted them to stay under temporary protected status. The unanimous opinion, written by Justice Elena Kagan, said current immigration law only permits those who were admitted lawfully to the U.S. to apply for permanent residency. [Continue Reading] **See also:** WaPo

CRIMINAL LAW

WSJ: **Federal Prosecutors Subpoena Material Related to Andrew Cuomo's Book,** Jimmy Vielkind and Corinne Ramey, June 7, 2021, 7:23 PM
Federal prosecutors have subpoenaed material related to New York Gov. Andrew Cuomo's recent memoir as part of their probe into Covid-19 deaths in the state's nursing homes, people familiar with the matter said. Prosecutors working for the U.S. Attorney's Office for the Eastern District of New York in Brooklyn asked for communications related to Mr. Cuomo's October 2020 book, "American Crisis," including contracts and materials used to pitch the book to publishers, the people said. [Continue Reading]

ANTITRUST

WSJ: **New York Senate Passes Antitrust Bill Targeting Tech Giants**, Ryan Tracy, June 7, 2021, 4:37 PM
The New York state Senate passed legislation Monday making it easier for plaintiffs to win antimonopoly lawsuits, in the latest state-led effort to rein in large technology companies in the absence of action by Congress. The antitrust

bill was opposed by business groups and backed by unions and other critics of corporate giants such as Amazon.com Inc. and Alphabet Inc.'s Google. To become law, it must also pass the state assembly and be signed by the governor. [...] Monday's 43-20 party line vote represented an incremental victory for advocates of tougher antitrust laws, who will seek to use it as a springboard to tougher laws in other states and at the federal level. [Continue Reading]

CRIMINAL JUSTICE/CORRECTIONS

Reuters: **Fleeing Texas inmates outsmarted jailers by placing dummies in bed,** Sarah N. Lynch, June 7, 2021, 4:48 PM
Security at a federal prison camp in the Texas city of Beaumont was so lax that four inmates managed to escape by placing dummies in their beds or having other prisoners pose as them, the U.S. Justice Department's internal watchdog said on Monday. Inspector General Michael Horowitz said his office uncovered a wide range of security failures at prison camps and satellite campuses of the Bureau of Prisons, from leaving doors unlocked or using locks that were susceptible to tampering, to having limited fencing or not enough video surveillance. [Continue Reading]

NATIVE AMERICAN AFFAIRS

KFOR-NBC (Oklahoma City, OK): **Cherokee Nation files 1000th case in Tribal court following McGirt ruling,** Kaylee Douglas, June 7, 2021, 5:19 PM
The Cherokee Nation has filed its 1000th case in Cherokee Nation District Court since the Supreme Court McGirt ruling and subsequent Hogner decision found that its reservation had never been disestablished, and that the state of Oklahoma had been improperly prosecuting cases outside of its jurisdiction for over a century. "Since Indian Country's victory in McGirt, the Cherokee Nation has made two priorities crystal clear: we will fight to protect every piece of our hard-earned sovereignty, and we will stand with victims and families to keep everyone on our reservations and our neighbors throughout Oklahoma safe," said Cherokee Nation Attorney General Sara Hill. [Continue Reading]

ADMINISTRATION

Reuters: **Harris takes on graft in Guatemala and tells migrants 'do not come'**, Nandita Bose and Sofia Menchu, June 7, 2021, 8:28 PM
U.S. Vice President Kamala Harris said on Monday she had "robust" talks with Guatemalan President Alejandro Giammattei on fighting corruption to deter immigration from Central America and bluntly warned migrants to not come to the United States. [Continue Reading] **See also:** Daily Caller, NBC, NYT, Politico, WaPo

NETWORK EVENING NEWS LINEUP: JUNE 7, 2021

***ABC:* World News Tonight with David Muir**
***CBS:* Weekend News with Norah O´Donnell**
***NBC:* Nightly News with Lester Holt**

- The federal government has recovered millions of dollars in cryptocurrency paid in ransom to cybercriminals whose attack prompted the shutdown of the country's largest fuel pipeline and gas shortages across the southeastern US last month, the Department of Justice announced Monday. On May 8, Colonial Pipeline paid a ransom worth roughly $4.3 million in bitcoin to the Russia-based hacking group known as DarkSide, which had used malicious software to hold the company hostage. [ACB, CBS, NBC]
- Vice President Harris is in Guatemala City on Monday to kick off the first foreign trip of her time in office, a two-day mission aimed at trying to strengthen ties with Guatemala and Mexico and tackle tough and longstanding problems such as corruption, violence and poverty, some of the issues behind the record number of migrants from Central America seeking asylum at the US border in recent months. [ABC, CBS, NBC]
- Two suspects are being held on $1 million bail in connection with the fatal shooting of six-year-old Aiden

Leos, who was killed last month on his way to kindergarten. Police believe the shooting may have been a road rage incident. [ABC, CBS, NBC]