From: Hornbuckle, Wyn (PAO)
Subject: RE: TIME SENSITIVE - GAO 104362: DOJ/OPA Request #1
To: Smith, Stephanie K. (JMD)
Sent: December 14, 2021 6:22 PM (UTC-05:00)
Attached: FY22_ALL_STAFF-#147374-v6-104362__QUESTIONS_FOR_DOJ_OPA_#1_-_QUESTIONS_ON_CHINA_INITIATIVE_-_11_8_21.docx

Stephanie – See OPA responses in the attached.

Please let me know if you have any additional questions.

Best regards and thanks for your patience,

Wyn Hornbuckle
Deputy Director, Office of Public Affairs
U.S. Department of Justice
O:(b) (6)
M:(b) (6)

From: Smith, Stephanie K. (JMD) (b) (6)
Sent: Tuesday, December 14, 2021 4:59 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: TIME SENSITIVE - GAO 104362: DOJ/OPA Request #1

Thank you for the update Wyn.

Stephanie Kennedy Smith
Audit Liaison Specialist
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, N.E.
2 Con – (b) (6)
Washington, D.C. 20530
(b) (6)

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Tuesday, December 14, 2021 3:04 PM
To: Smith, Stephanie K. (JMD) (b) (6)
Subject: Re: TIME SENSITIVE - GAO 104362: DOJ/OPA Request #1

Stephanie
This is on my list for today. I will have a response completed by the end of the week if not earlier.
Apologies for the delay

Sent from my iPhone

On Dec 14, 2021, at 2:51 PM, Smith, Stephanie K. (JMD) (b) (6) wrote:

Good Afternoon,

Do you happen to have any idea when I can expect OPA's response? Since we are passed the deadline, I need to provide the GAO team with an approximate date/time when they can expect to receive OPA's response. Thanks…

Stephanie Kennedy Smith
Audit Liaison Specialist
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, N.E.
2 Con - (b) (6)
Washington, D.C. 20530
(b) (6)

From: Smith, Stephanie K. (JMD) (b) (6)
Sent: Monday, December 13, 2021 11:04 AM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: TIME SENSITIVE - GAO 104362: DOJ/OPA Request #1
Importance: High

Good Morning,

I'm checking on the status of this request. Please provide an update. The deadline has passed.
I need to provide an update to GAO. If you would rather discuss this matter over the phone, please let me know your phone number and a good time to call. Thank you.

Stephanie Kennedy Smith
Audit Liaison Specialist
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, N.E.
2 Con - (b) (6)
Washington, D.C. 20530
(b) (6)

From: Smith, Stephanie K. (JMD) (b) (6)
Sent: Friday, November 12, 2021 1:40 AM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: GAO 104362: DOJ/OPA Request #1
Importance: High

Good Morning,

I am an audit liaison working in the JMD, audit liaison group, I am currently working on an engagement concerning *Safeguarding U.S. Research from Unlawful Transfer to China, 104362*. During the audit, NSD mentioned that OPA had information on this topic. Which prompted GAO to submit the above request for information (RFI) and question set. Please let me know who on the OPA staff I should work with to get these questions answered and the RFI completed. Written response is acceptable. After reviewing the questions and RFI, please let me know if you have questions or concerns. Please note, OPA's response is due to me NLT 12/3/21.

Stephanie Kennedy Smith
Audit Liaison Specialist
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, N.E.
2 Con - (b) (6)
Washington, D.C. 20530
(b) (6)

104362: Safeguarding Sensitive U.S. University Research from Transfer to China
Follow-up on DOJ/OPA China Initiative Investigations – November 8, 2021

In responses to previous questions, DOJ/NSD referred us to DOJ/OPA on several lines of inquiry related to information about the China Initiative included on DOJ's website and mentioned by DOJ spokespersons.

1. Please describe DOJ/OPA's role in the China Initiative, including maintaining online information for the China Initiative such as https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

   OPA communicates with and responds to the national news media, and generally supports official messaging through speeches, press conferences, and events for all DOJ components and principals, including the National Security Division. This includes providing statements, press releases and information about the China Initiative to the news and general public on demand. OPA has maintained a China Initiative Fact Sheet on justice department website, where it has kept information about ongoing prosecutions and adjudicated cases with a nexus to the PRC.

2. With respect to the latest China Initiative Year-in-Review (https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20) and the other online information about China-related cases:

   a. How often and using what criteria does DOJ add cases to the public China Initiative web pages?

      Periodically as developments occur in specific cases, such as a trial conviction or sentencing, or a case dismissal. Due to a number of developments that occurred over the summer and early fall, OPA substantially updated the website in November 2021.

   b. What information about each case is available to OPA for use in compiling the Year-in-Review and creating the content for the China Initiative web pages?

      Final press releases are the basis for updating the site, and other content cleared through the National Security Division for release, such as the 2018 Year in Review press release: https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20

   c. How does OPA determine what investigation details to include in the case examples posted online?

      Like all press materials we handle, they are based on what is publicly available in the court record regarding prosecutions, and do not include information from ongoing investigations, in accordance with Justice Department guidelines. (Title 1, Section 7)

      1-7.000 - Confidentiality and Media Contacts Policy | JM | Department of Justice

   d. What input or guidance, if any, has OPA received regarding which China Initiative cases to include on DOJ's public website, and from what DOJ elements does such instruction come (e.g., NSD, FBI, etc.)?

      NSD

3. We noted that DOJ's public China Initiative web pages seem to include outdated information on certain cases (based on our review of publicly reported information and case documents associated with related prosecutions). To what extent, if at all, does OPA update original online postings to reflect developments or outcomes (e.g., convictions, acquittals, dismissals)?

    a. If DOJ does update online information, how often and for what reasons might OPA make such updates for previously-listed cases?

    Periodically as developments occur in specific cases, such as a trial conviction or sentencing, or a case dismissal. Due to a number of developments that occurred over the summer and early fall, OPA substantially updated the website in November 2021. This also included consolidating multiple releases on the same case to reflect the most recent information. It also including removing erroneous information, including one case that was unrelated to the PRC that had been listed in error, and cases where there was a dismissal or acquittal. NOTE: These releases remain accessible on DOJ's website and include banners that provide the updated information, but they no longer appear on the China initiative Fact Sheet. Here's an example: Researcher at University Arrested for Wire Fraud and Making False Statements About Affiliation with a Chinese University | OPA | Department of Justice

4. Does OPA plan to release a year in review for 2020/21 as it did for 2019/20? yes.

    a. When is the release planned? TBD, year end

    b. How did/will OPA determine what China Initiative efforts to highlight in the 20/21 year in review? TBD

5. DOJ Spokesman Wyn Hornbuckle statement(s) related to the July 2021 dismissal(s) of China Initiative cases has been reported by various media outlets. Please provide the full text of these and any other DOJ statements or press releases by Mr. Hornbuckle or other DOJ spokespersons that are related to acquittals or dismissals of China Initiative prosecutions. *(See request item #2.)*

    7/23/21

    - "In all of our prosecutions, the Department of Justice evaluates the merits of a case as it prepares for trial. Recent developments in a handful of cases involving defendants with alleged, undisclosed ties to the People's Liberation Army of the People's Republic of China have prompted the Department to re-evaluate these prosecutions, and we have determined that it is now in the interest of justice to dismiss them. The Department continues to place a very high priority on countering the threat posed to American research security and academic integrity by the PRC government's agenda and policies. We remain fully committed to enforcing the criminal laws that protect the intellectual property, critical and emerging technology, and other national assets essential to our nation's security and prosperity."

    8/26/21

- "The Department is dedicated to countering unlawful PRC government efforts to undermine America's national security and harm our economy. As we work to protect the United States against one serious threat – the sophisticated PRC targeting of our institutions and individuals whose political views pose a challenge to the regime – we are also mindful of our responsibility to combat another serious threat: the substantial rise in hate crimes and bias targeting the Asian American Pacific Islander community. We take seriously concerns about discrimination and are committed to working with affected communities to build upon and improve the Department's efforts."

9/10/2021

- Regarding a decision by a federal judge in Knowxville to acquit the case against University of Tennessee Professor Anming Hu:

  "We respect the court's decision, although we are disappointed with the result"

6. What, if any, changes does DOJ envision for the scope or mission of the China Initiative or how it will be presented on DOJ's public website? TBD

Hornbuckle Statement 12/13/21 Update:

- "Consistent with the Attorney General's direction, the Department is reviewing our approach to countering threats posed by the PRC government. We anticipate completing the review and providing additional information in the coming weeks."

From: McGowan, Ashley L. (PAO)
Subject: RE: PRC related case updates on the website
To: Hornbuckle, Wyn (PAO); Shevlin, Shannon (PAO)
Sent: November 15, 2021 3:05 PM (UTC-05:00)

Thanks – updates have been made to all 4 releases.

From: Hornbuckle, Wyn (PAO) [redacted]
Sent: Monday, November 15, 2021 2:58 PM
To: McGowan, Ashley L. (PAO) [redacted]; Shevlin, Shannon (PAO)
[redacted]
Subject: RE: PRC related case updates on the website

Looks fine thanks

From: McGowan, Ashley L. (PAO) [redacted]
Sent: Monday, November 15, 2021 2:26 PM
To: Shevlin, Shannon (PAO) [redacted]; Hornbuckle, Wyn (PAO) [redacted]
Subject: RE: PRC related case updates on the website

Thanks for re-flagging the dismissal/acquittal language – I had missed that and thought all the updates were for the fact sheet. I'm making the changes now.

Here's the language I'm adding to these releases – please review and let me know if there are any edits:

SDOH dismissed charges: Former Cleveland Clinic Employee and Chinese "Thousand Talents" Participant Arrested for Wire Fraud | OPA | Department of Justice

UPDATE

The government dismissed all charges alleged in the indictment described in the press release below.

The PLA visa cases dismissed by the gov:
Chinese National Charged with Destroying Hard Drive During FBI Investigation into the Possible Transfer of Sensitive Software to China | OPA | Department of Justice
Researchers Charged with Visa Fraud After Lying About Their Work for China's People's Liberation Army | OPA | Department of Justice

UPDATE

The government dismissed all charges alleged in the indictment described in the press release below.

Anming Hu case. Acquitted by the court: https://www.justice.gov/opa/pr/researcher-university-arrested-wire-fraud-and-making-false-statements-about-affiliation

UPDATE

The defendant in this case, Anming Hu, was acquitted by the court of the charges alleged in the indictment described in the press release below.

From: Shevlin, Shannon (PAO) [redacted]

Sent: Monday, November 15, 2021 2:11 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6)
Subject: RE: PRC related case updates on the website

Thanks, Wyn! Making those changes to the China Initiative Fact Sheet and will send you a revised version.

Ashley, let me know if you need support on the dismissal/acquittal language.

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Monday, November 15, 2021 1:43 PM
To: Shevlin, Shannon (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6)
Subject: RE: PRC related case updates on the website

Bumping this up on your radars when we can get to it

From: Hornbuckle, Wyn (PAO)
Sent: Sunday, November 14, 2021 10:05 PM
To: Shevlin, Shannon (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6)
Subject: PRC related case updates on the website

Hey Shannon – let's discuss the China Initiative website updates in the am. These are the main changes that need to be made asap:

Remove references to John Demers chairing the initiative, as he has left the department

We should add the following trial conviction:
The Xu conviction from Nov. 5 https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets

These items should be removed from the China initiative case examples (but should remain accessible on the justice.gov website under "News"). For those dismissed/acquitted cases that remain accessible on the website, we need to insert a disclaimer that the cases were dismissed/acquitted. We can talk more about the exact language tomorrow. Ashley can also walk you through how we do that.

SDOH dismissed charges: Former Cleveland Clinic Employee and Chinese "Thousand Talents" Participant Arrested for Wire Fraud | OPA | Department of Justice

The PLA visa cases dismissed by the gov:
Chinese National Charged with Destroying Hard Drive During FBI Investigation into the Possible Transfer of Sensitive Software to China | OPA | Department of Justice
Researchers Charged with Visa Fraud After Lying About Their Work for China's People's Liberation Army | OPA | Department of Justice

Anming Hu case. Acquitted by the court: https://www.justice.gov/opa/pr/researcher-university-arrested-wire-fraud-and-making-false-statements-about-affiliation

Wildlife case: Chinese Man Extradited for Financing Turtle-Trafficking Ring | OPA | Department of Justice (this was not dismissed, just has nothing to do with the PRC, so should just be removed)

Happy to discuss in the am,

Wyn Hornbuckle
Deputy Director, Office of Public Affairs
U.S. Department of Justice
O:(b) (6)
M:(b) (6)

From: Hornbuckle, Wyn (PAO)
Subject: RE: China Initiative and NSD website
To: (b)(6) Marc Raimondi
Cc: Pietranton, Kelsey (PAO)
Sent: November 9, 2021 4:00 PM (UTC-05:00)

Thanks Marc. Yes, we are due for some updates, and appreciate the flags. Missing you….:)

From: (b)(6) Marc Raimondi
Sent: Tuesday, November 9, 2021 3:11 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Cc: Pietranton, Kelsey (PAO) (b) (6)
Subject: [EXTERNAL] China Initiative and NSD website

Wyn (Kelsey for awareness), Just had a call from MIT Technology review on the China Initiative. She had questions about the origin, types of cases, etc. I walked he through the history of DOJ cases involving PRC actors and talked to her about how there is not a charge of China initiative, but rather the initiative was focused on China related economic and pollical malfeasance and non-traditional collection of information. I walked her through a bunch of the cases on the China Initiative Fact sheet she asked about. She seemed fixated on the notion that only 17 of the 75 cases on the CA fact sheet were for economic espionage. I conveyed that the initiative was certainly not limited to charges of economic espionage and used the Ransomware task force as an Examples. I told her if there was a money laundering charge of someone affiliated with REvil, its going to get wrapped up as Ransomware Task Force related case and communicated as such. Same thing here, if there is a trade secret case with a nexus to China, we would count it. I then explained the difference between Trade secret theft and economic espionage.

She said her and her colleagues are concerned about the turtle case and wanted to know why it was under the China Initiative fact sheet. I was surprised to see it too. This one must have slipped by me. I recommend it be removed from the China fact sheet. It is at https://www.justice.gov/opa/pr/chinese-man-extradited-financing-turtle-trafficking-ring

They also asked why the MIT case out of Boston from February 12th wasn't on the sheet. I told her it was probably because we had a lot of other things going on January 12th. But I would suggest asking Jay Bratt about that case specifically (call me for more specifics). You may revisit posting it based on time passed, I certainly think it fits the mold to go there.

I would also suggest you review the other releases since then and consider posting more cases, like the Ohio conviction of the MSS officer in Ohio last week. Looks like this hasn't been updated for a few months. Shannon used to do it every Friday.

Lastly, John Demers is still listed as the head of it. May want to strike his name and just stick to the positions. Then again, there may be a lot more going on that I am unaware of regarding the program and branding of it.

While I am at it, this page still has John Demers on it. May want to flag it for NSD to get Matt's photo and message up there. https://www.justice.gov/nsd/external-engagement

And lastly, I noted this page hasn't been updated since 2017 when I was at the White House and you were covering for me: https://www.justice.gov/nsd/external-engagement. Luckily, it is correct again. You may want to put your email in there as you don't have access to the NSD public email account (although you can get access if you ask, I used to go through it and found some mis sent media inquires).

Feel free ignore all my recommendations

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE
Thursday, December 10, 2020

Chinese Man Extradited for Financing Turtle-Trafficking Ring

A Chinese citizen was extradited from Malaysia to the United States today to face charges for money laundering.

Kang Juntao, 24, of Hangzhou City, China, was charged in February 2019 with financing a nationwide ring of individuals who smuggled at least 1,500 protected turtles out of the United States valued at $2,250,000.

"The Department of Justice is committed to prosecuting criminals who abuse the U.S. financial system to fund their illegal enterprises," said Principal Deputy Assistant Attorney General Jonathan D. Brightbill of the Justice Department's Environment and Natural Resources Division. "I thank the U.S. Fish and Wildlife Service for their extraordinary efforts in this case to support the Environment and Natural Resources Division's mission to protect America's wildlife."

"Wildlife trafficking is a serious crime that impacts imperiled species at home and abroad," said Aurelia Skipwith, Director of the U.S. Fish and Wildlife Service (USFWS). "The Trump Administration is committed to the conservation of wildlife. I would like to thank the U.S. Department of Justice and our various law enforcement partners for their assistance with this case. By working together, we can protect our nation's wildlife for future generations."

According to the indictment, from June 12, 2017, through Dec. 3, 2018, Kang allegedly purchased turtles in the United States and arranged for them to be smuggled to associates in Hong Kong. He sent money through U.S. banks, including one in New Jersey, to pay for the turtles and their illegal shipments. The turtles would then be sold on the Asian pet trade black market for thousands of dollars each, depending on their sex, coloring, and age.

The United States, Malaysia, China, and approximately 181 other countries are signatories to the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES). CITES is an international treaty that restricts trade in species that may be threatened with extinction.

Kang allegedly trafficked in five turtle species protected by the treaty. The eastern box turtle (*Terrapene carolina carolina*), the Florida box turtle (*Terrapene carolina bauri*), and the Gulf Coast box turtle (*Terrapene carolina major*) are subspecies of the common box turtle (*Terrapene carolina*) and have been listed in CITES since 1995. The spotted turtle (*Clemmys guttata*) is a semi-aquatic turtle listed in CITES as of 2013. The wood turtle (*Glyptemys insculpta*) has been protected under CITES since 1992.

The indictment further alleges that Kang sent money via PayPal to the United States to purchase turtles from sellers advertising on social media or reptile trade websites. These suppliers then shipped the turtles to middlemen across five different states. The middlemen were typically Chinese citizens who entered the country on student visas. Kang paid and instructed these intermediaries to repackage the turtles in boxes with false labels for clandestine shipment to Hong Kong. The turtles were inhumanely bound with duct tape and placed in socks so as not to alert customs authorities. Neither Kang nor his associates declared the turtles to U.S. or Chinese customs or obtained the required CITES permits.

The Royal Malaysia Police arrested Kang on Jan. 23, 2019, at Kuala Lumpur International Airport on a request submitted by the United States for his provisional arrest with a view to extradition. An extradition request was subsequently submitted on March 5, 2019, pursuant to the Extradition Treaty between the Government of the United States of America and the Government of Malaysia. Kang's extradition was finalized in September 2020 and he was surrendered to the United States Wednesday as provided by the extradition treaty. The United States is grateful to the Minister of Home Affairs of Malaysia, the Attorney General of Malaysia and the Transnational Crimes Unit, Prosecution Division, Attorney General's Chambers for their steadfast cooperation and support in the litigation of

the extradition request. We also thank the U.S. Justice Department's Office of International Affairs, U.S. Immigration and Customs Enforcement's Homeland Security Investigations Malaysia Attaché, the Regional Security Office, Bureau of Diplomatic Security, U.S. Department of State, and the Consular Section of the U.S. Embassy in Kuala Lumpur for providing invaluable assistance in supporting the extradition and coordinating the return of Kang to the United States.

An indictment is merely an allegation, and the defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The USFWS conducted the investigation and escorted Kang to the United States. The government is represented by Trial Attorneys Ryan Connors and Lauren Steele of the Environment and Natural Resources Division's Environmental Crimes Section.

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.

Attachment(s):
Download Kang Indictment
Topic(s):
Wildlife
Component(s):
Criminal - Office of International Affairs
Environment and Natural Resources Division
Press Release Number:
20-1336

From: Shevlin, Shannon (PAO)
Subject: RE: China initiative questions
To: Hickey, Adam (NSD); (b)(6), (b)(7)(C) per NSD (NSD); Bratt, Jay (NSD); (b)(6), (b)(7)(C) per NSD (NSD)
Cc: Hornbuckle, Wyn (PAO); Pietranton, Kelsey (PAO)
Sent: November 9, 2021 3:08 PM (UTC-05:00)
Attached: MG on China Initiative.docx, Bloomberg China Qs v2 clean.docx, Bloomberg China Qs v2.docx

Thanks, all. I've added your edits and updated the language. Redlined and clean versions attached.

Also including the AG's most recent testimony at DOJ oversight committees a few weeks ago if that would be helpful.

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Tuesday, November 9, 2021 8:20 AM
To: (b)(6), (b)(7)(C) per NSD Shevlin, Shannon (PAO) (b) (6); Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) (b) (6); Pietranton, Kelsey (PAO) (b) (6)
Subject: RE: China initiative questions

Those are great, thanks. Shannon, are you able to clean this up and send around again for us to look at the final? I want to make sure the accomplishments at the top are complete. (b)(6), (b)(7)(C) per NSD (in FIRS) and Jay (b)(6), (b)(7)(can help you with that.

From: (b)(6), (b)(7)(C) per NSD
Sent: Monday, November 08, 2021 8:30 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Shevlin, Shannon (PAO) (b) (6); Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) (b) (6) Pietranton, Kelsey (PAO) (b) (6)
Subject: RE: China initiative questions

(b)(5) per NSD .

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >
Sent: Monday, November 8, 2021 5:53 PM
To: (b)(6), (b)(7)(C) per NSD Shevlin, Shannon (PAO) (b) (6); Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) (b) (6); Pietranton, Kelsey (PAO) (b) (6) >
Subject: RE: China initiative questions

Thanks, (b)(6), (b)(7) .(b)(5) per NSD

Adam

From: (b)(6), (b)(7)(C) per NSD
Sent: Monday, November 8, 2021 5:09 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >; Shevlin, Shannon (PAO) (b) (6); Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) (b) (6); Pietranton, Kelsey (PAO) (b) (6)
Subject: RE: China initiative questions

A few additional comments.

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Monday, November 8, 2021 4:35 PM
To: Shevlin, Shannon (PAO) (b) (6) ; Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD ; (b)(6), (b)(7)(C) per NSD >
Cc: Hornbuckle, Wyn (PAO) <(b) (6) Pietranton, Kelsey (PAO) <(b) (6) (b)(6), (b)(7)(C) per NSD
Subject: RE: China initiative questions

Thanks, Shannon. I think these are pretty good, by and large, but here are my suggestions. CES should also take a look. (b)(6), (b)(7)(C) per NSD

Adam

From: Shevlin, Shannon (PAO) <(b) (6)
Sent: Monday, November 8, 2021 2:29 PM
To: Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD ; Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD ; (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) <(b) (6) Pietranton, Kelsey (PAO) <(b) (6)
Subject: China initiative questions

Hi NSD,

We received some questions from Bloomberg last week for a story on the China Initiative. They plan to issue a long feature in Businessweek magazine that contains the data analysis in Question 4 and detailed information about individual cases.

See questions and first go at answers in the attached word document. We used Wyn's topline messaging to draft most of the responses, but would love your feedback and additions, especially on the technical and case-specific items. Please let me know if there are additional resources or you'd like further support drafting answers.

Thanks!
Shannon

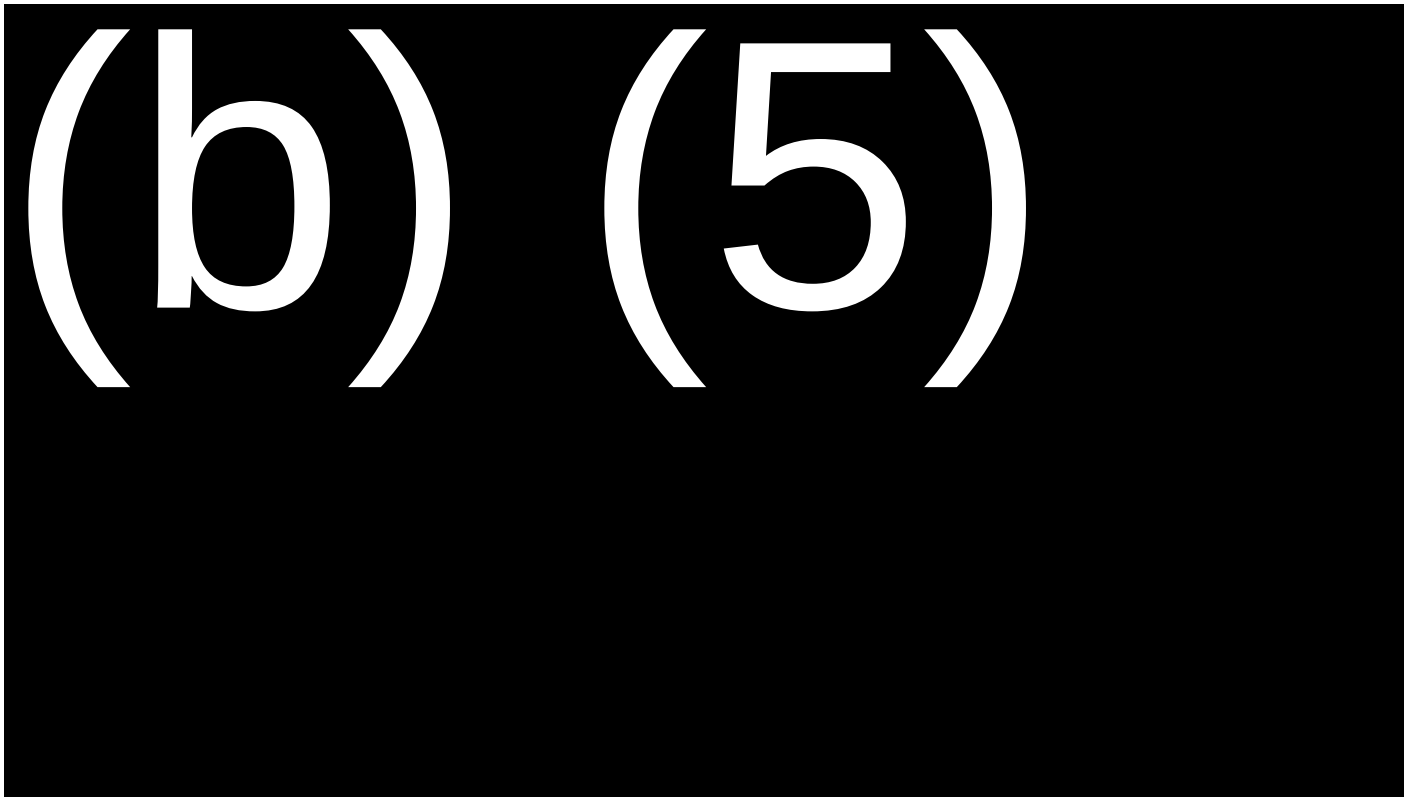
Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

1. Can you please provide a definition for China Initiative cases and a list of cases that have been brought or prosecuted as China Initiative cases? If a list is not available, can you provide a total number of China Initiative cases?

(b) (5)

2. What does the DOJ consider the biggest successes of the China Initiative? What are its failures?

(b) (5)



3. Defense attorneys, Asian-American groups, and members of Congress (Sen. Blackburn) have accused the DOJ of incompetence and/or overzealousness in bringing prosecutions that have resulted in numerous dropped cases and the directed verdict for Prof. Anming Hu at UTK. What is the DOJ's response?

4. A Bloomberg analysis of the 50 cases posted on the China Initiative page of the DOJ that have been brought or unsealed since the announcement of the Initiative on Nov. 1, 2018, (20 cases listed there pre-date the announcement of the China Initiative) finds that 38% are of researchers or professors charged with fraud or visa fraud; 20% are EEA; 18% concern illegal exports/sanctions violations/duties evasion; 16% involve hacking or cyber-intrusion (a couple of these overlap with EEA cases); actual espionage is charged in 3 cases.

Do you have any objections to this finding, and if so, could you provide your supporting data with cases and links?

5. Does DOJ have any further response to the criticism that the China Initiative has devolved into racial profiling -- that it starts out by targeting people with China ties (who are primarily Chinese or Chinese-American) and tries to find out if they committed crimes, rather than starting with crimes and finding who did them -- in addition to Merrick Garland's responses to members of Congress in two appearances in October?

(b) (5)

6. How long will Matt Olsen take to complete the review of the China Initiative? What is expected to happen after this review is completed?

7. Why are some cases, such as Gang Chen of MIT, not posted as China-related cases on the China Initiative web page? Does it mean they are not considered part of the China Initiative? Was his case posted and then later removed?

https://www.justice.gov/usao-ma/pr/mit-professor-arrested-and-charged-grant-fraud

(b) (5)

8. Why were some cases, such as Dr. Qing Wang, dropped from the list of China-related cases on the China Initiative web page? How many such cases have been removed, in addition to his?

https://www.justice.gov/opa/pr/former-cleveland-clinic-employee-and-chinese-thousand-talents-participant-arrested-wire-fraud

9. How many China-related cases under the China Initiative are currently under investigation or prosecution but have not yet been announced or remain sealed? Merrick Garland told Sen. Blackburn that China-related cases are still proceeding in line with FBI Director's Wray's previous comment that counter-intelligence cases involving China are being opened every 10 hours. Is that still the case?

(b) (5)

10. Regarding the case of Feng "Franklin" Tao in Kansas City, since it has many similarities to the Anming Hu case which resulted in an embarrassing directed verdict, is the DOJ confident about bringing the Tao case? It is scheduled for trial Dec. 6. Since the defense has said the FBI acted with malfeasance in obtaining a warrant on the basis of lies from an unreliable informant, do you have any comment on the decision by prosecutors to bring this case anyway?

(b) (5)


(b) (5)

Oct. 21:

Rep. Ted Lieu: I'd like to now talk about a case brought under the China Initiative that happened under your watch the case of Professor Anming Hu, who was also wrongfully accused of spying for China. Evidence against him was so flimsy that a federal judge dismissed the case under Rule 29 motion. I'm a former prosecutor, I know that those motions are rarely, if ever, granted. The judge found that even viewing all the evidence in the light most favorable to the prosecution, no rational jury could conclude that the defendant violated the law.

If we look at one of the darkest periods of our nation's history over 100,000 Americans who happened to be of Japanese descent were interned because our government could not figure out the difference between the Imperial Army of Japan and Americans who happen to be of Japanese descent, asking the Department not to repeat that similar type of mistake. And I'm asking you if you will look into the China initiative to make sure it's not putting undue pressure on the department to wrongfully target people of Asian descent.

MG: Internment of Japanese Americans… Terrible stain on American people and on the American government and on American history. I can assure you with that kind of racist behavior will not be repeated. There is a new Assistant Attorney General for the National Security Division who is pending confirmation. I am sure that when he is confirmed, which hopefully will be in the next few days. Maybe in the next few weeks. We'll review all the activities in the department and his division and make a determination of which cases to pursue and which ones not. I can assure you that cases will not be pursued based on discrimination, but only on facts justifying them.

Lieu: Mr. Chair, may I ask unanimous consent to enter three documents into the record? The first is a study I referenced called *Racial Disparities and Economic Espionage Act Prosecutions: a Window into the new Red Scare* dated September 21, 2021. The second is an article entitled *Professor Acquittal: is China Initiative Out of Control*, dated September 25, 2021. The final document is a letter from 177 Stanford faculty outlining why the China initiative is discriminatory and harms American competitiveness dated September 8, 2021.

Oct. 27:

Sen. Mazie Hirono: You've been asked before, I think in the House hearing, about the China initiative. If we end the China Initiative, will we no longer go after economic espionage and IP threats by China?

MG: There are two issues that we always have to keep upper most in our minds. One is that the people's republic of china is a serious threat to our intellectual property. They represent a serious threat with respect to espionage. They represent a serious threat with respect to cyber incursions and ransomware in the united states. And we need to protect the country against this. And we will and we are in cases in that regard. The other thing that always has to be remembered is that we never investigate or prosecute, based on ethnic identity. On what country a person is from or came from or their family.

Hirono: And the reason I ask about the china initiative is under the previous administration, which instituted the so-called initiative, there appears to have been racial profiling, which basically ruined the lives of a number of Chinese people. I want to give an example. The Justice Department, previous administration, dragged Dr. Anming Hu, a professor at the University of Tennessee, through a two-year espionage investigation, causing him to lose his job. At the end of the investigation, DOJ lacked any

evidence of espionage and instead, charged the doctor with wire fraud and false statements for apparently failing to disclose his association with a Chinese university on a NASA grant application. His trial ended in a mistrial, after which a juror said she was, quote, pretty horrified by the lack of evidence, end quote. When DOJ sought new trial they granted the motion for acquittal, finding no harm to NASA and no evidence Dr. Hu knew NASA's funding restriction applied to Chinese universities. So, I would say, regardless whether we have something called the Chinese initiative, you have no intention to not pay attention to espionage and other bad acts by China. I say we should get rid of this, what? This initiative that results in racial profiling. Thank you, Mr. Chairman.

Sen. Marsha Blackburn: Give me an update – what's the status of the China Initiative at DOJ?

MG: We regard People's Republic of China as an extraordinarily serious and aggressive threat to our intellectual property, to our universities.

Blackburn: You're stonewalling me on that. We all know they're an aggressive threat

MG: We continue to investigate the PRC efforts

Blackburn: Do you see them as an adversary?

MG: I see them as adversarial with respect to ransomware, with respect to hacking, with respect to counterintelligence, respect to counterespionage.

Blackburn: Over the last 9 months, several espionage prosecutions of researchers have been dropped or charges have been dismissed, including those of a UT professor at UT Knoxville. This is in spite of the fact that Director Wray recently testified that the FBI opens a new Chinese espionage investigation every 12 hours. So, are there apparent failures of the initiative, is it a lack of leadership? Or is it a compromise position with the administration? Is it incompetence?

MG: Every case is evaluated on its own with respect to the law and the facts. We continue to open cases involving the People's Republic of China Daily as the as the Director said, we will not in any way let up our concerns about China.

Blackburn: I want to move on. Glad to know you're not going to go soft on China because this administration is going soft on China.

From: Hornbuckle, Wyn (PAO)
Subject: RE: in the interests of time
To: Newman, David A. (ODAG)
Cc: Hickey, Adam (NSD); Bratt, Jay (NSD)
Sent: August 24, 2021 1:37 PM (UTC-04:00)
Attached: CHINA INTIATIVE TOP LINE MESSAGES AND BACKGROUND clean version 8.24.21.docx

Here's the updated backgrounder and on record statement, which has been cleared by the NSC:

From: Newman, David A. (ODAG) <(b) (6)
Sent: Tuesday, August 24, 2021 1:33 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Cc: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
Subject: Re: in the interests of time

Thank you. Very sorry.

On Aug 24, 2021, at 1:03 PM, Hornbuckle, Wyn (PAO) <(b) (6) wrote:

I'll try and move it back an hour

From: Newman, David A. (ODAG) <(b) (6)
Sent: Tuesday, August 24, 2021 1:02 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Cc: Hornbuckle, Wyn (PAO) <(b) (6) Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
Subject: Re: in the interests of time

I'm truly sorry. But I am needed in an AG briefing. Would it be possible to push both the prep and the interview back an hour (so, 2pm and 2:30pm). If not, I will step away at 1:20 to do a quick prep and then be on this.

On Aug 24, 2021, at 12:55 PM, Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD > wrote:

Seems fine to me.

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Tuesday, August 24, 2021 10:22 AM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Newman, David A. (ODAG) <(b) (6)
Subject: RE: in the interests of time

Planning to share the following on background to Ellen later this am before our call, that way we don't need to waste time answering these. If there are some you'd rather handle during the call than in writing let me know. This would be on background, attributable to the Justice Department

---

From: Nakashima, Ellen <(b) (6)
Sent: Monday, August 23, 2021 2:02 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Cc: Nakamura, David <(b) (6)
Subject: in the interests of time

Wyn,

Can you provide some of these stats so that we can focus our discussion with David and Adam on programmatic issues?

Can you quantify specifically how many investigations have been brought under the China Initiative since Nov. 2018 and how many have resulted in criminal charges? How many investigations have been concluded without charges? How many deal with academics and scientific researchers?

- Since November 2018, we have brought or resolved nine economic espionage prosecutions and seven theft of trade secrets cases with a nexus to the PRC. We also have brought 12 matters involving fraud on universities and/or grant making institutions.

There have been four convictions/pleas in the economic espionage/theft of trade secret matters, and four in academic fraud cases. We do not track the number of these sorts of cases that we decline or close without charges.

FBI Director Wray said last year that agents are opening a new counterintelligence case related to China every 10 hours and that about half of the FBI's nearly 5,000 investigations related to China. Is that still the case? If not, can you update those numbers?

- How the FBI defines an investigation, which can be a purely intelligence investigation, is not the same as how DOJ defines an active grand jury investigation. We do not disclose the latter number.

Thanks!
Ellen and David

From: Nakamura, David <(b) (6)
Sent: Friday, August 20, 2021 6:15 PM
To: Hornbuckle, Wyn (PAO) <(b) (6) Nakashima, Ellen <(b) (6)
Subject: RE: China initiative interview

Hi Wyn,

Thanks for this information. I don't see the Lu/Liu case included on DOJ's list of China Initiative case examples here https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (I did see the separate press release

the department issued here https://www.justice.gov/usao-wdok/pr/husband-and-wife-working-university-arrested-wire-fraud-involving-department-energy)

- As to the Lu/Liu case, the original indictment charged them with straightforward fraud, stemming from their using university and grant money for personal expenses. Although charges were later added in a superseding indictment, they ultimately agreed to plead guilty to the original fraud conduct, so the case was not included on the list.

But some other cases are not listed on that first list of more than 70 cases, including the charges against MIT professor Gang Chen and the Qing Wang case, which advocates who track the initiative said was removed from the list after the case was dropped. Can you please help us understand what this list is: https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related Is it supposed to be an exhaustive list of China Initiative cases or just representative samples? And why is the Gang Chen case not included? How many China-related cases since Nov. 2018 are not included on that list?

- It's intended to be a comprehensive list of cases that implicate PRC government policies and practices, but it is compiled by humans so subject to some degree of error. The case against Gang Chen is a simple oversight on our part, and will be added. Also, re Hao Zhang we include cases that remained pending on or after the announcement of the initiative. We have long been enforcing laws against economic espionage, computer hacking, proliferation, etc., and we apply the same standard (in terms of proof) in deciding to charge cases before and after the initiative was announced.

If it's the latter, how are you deciding which cases to include and why would DOJ take down the Qing Wang case after the charges were dropped?

- The Qing Wang case was removed after the case was dismissed. When a case is dismissed, (b) (5) .

One other question: The Hao Zhang case appears to have begun in 2015 when he was indicted. He was found guilty by a judge and sentenced in 2020. You are including that in cases brought after 2018 – just for our understanding, could you explain why? See above

Thank you,
Dave

David Nakamura
Washington Post Staff Writer
(b) (6)
o. (b) (6)
c. (b) (6)
Twitter: @davidnakamura

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Friday, August 20, 2021 5:46 PM
To: Nakamura, David <(b) (6) Nakashima, Ellen <(b) (6)

Subject: RE: China initiative interview

Some facts and answers to questions raised:

Since November 2018, we have brought or resolved nine economic espionage prosecutions and seven theft of trade secrets cases with a nexus to the PRC. We also have brought 12 matters involving fraud on universities and/or grant making institutions. Of these 12:

- We have obtained four guilty pleas/convictions.
  - Lewis (NDWV)
  - Zheng (SDOH)
  - Lu and Liu (although not to the charges involving Talent Plan conduct)
- There has been one dismissal – Wang (NDOH)
- There has been one trial, which resulted in a hung jury – Hu (EDTN)

What are the overall goals and outcomes of the China Initiative? The one-year recap contains a substantive description of elements of the China Initiative.
https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20 [justice.gov]
To that we would add that protecting *all* U.S. persons—including Chinese nationals and other ethnic Chinese---from overreach/transnational repression by the Chinese state. (E.g., Telecom censorship prosecution [Zoom] and Foxhunt.)
https://www.justice.gov/opa/pr/nine-individuals-charged-superseding-indictment-conspiring-act-illegal-agents-people-s [justice.gov]
Goals of the China Initiative:

- Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
- Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities and the defense industrial base) that are being coopted into gaining access to U.S. technology and research contrary to U.S. interests;
- Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
- Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;
- Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- Implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- Identify opportunities to better address supply chain threats, especially those impacting the telecommunications sector, prior to the transition to 5G networks;
- Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;
- Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
- Evaluate whether additional legislative and administrative authorities are required

to protect our national assets from foreign economic aggression.

From: Nakamura, David <(b) (6)
Sent: Friday, August 20, 2021 3:47 PM
To: Nakashima, Ellen <(b) (6)
Cc: Hornbuckle, Wyn (PAO) <(b) (6)
Subject: Re: China initiative interview

I could be available then too just let me know thank you

Sent from my iPhone

On Aug 20, 2021, at 3:26 PM, Nakashima, Ellen <(b) (6) wrote:

Monday in the 3 – 5 p.m. window, I think.
Will you be able to send over the statistics and any other information today?

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Friday, August 20, 2021 2:34 PM
To: Nakashima, Ellen <(b) (6)
Cc: Nakamura, David <(b) (6)
Subject: RE: China initiative interview

CAUTION: EXTERNAL SENDER

I am working on this. We will have a response and hope to have some folks available for deep background. Do we have time to do it on Monday?

From: Nakashima, Ellen <(b) (6)
Sent: Friday, August 20, 2021 1:29 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Cc: Nakamura, David <(b) (6)
Subject: China initiative interview

Hi, Wyn,

Just checking back on timing.

Thanks,
Ellen

From: Hornbuckle, Wyn (PAO)
Subject: FW: in the interests of time
To: Ellen Nakashima (WaPo); Nakamura, David
Sent: August 24, 2021 12:07 PM (UTC-04:00)

In advance of our conversation, responses below are On Background, fine to paraphrase content and attribute to the Justice Department (no direct quotes):

From: Nakashima, Ellen <(b) (6)
Sent: Monday, August 23, 2021 2:02 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Cc: Nakamura, David <(b) (6)
Subject: in the interests of time

Wyn,

Can you provide some of these stats so that we can focus our discussion with David and Adam on programmatic issues?

Can you quantify specifically how many investigations have been brought under the China Initiative since Nov. 2018 and how many have resulted in criminal charges? How many investigations have been concluded without charges? How many deal with academics and scientific researchers?

- Since November 2018, we have brought or resolved nine economic espionage prosecutions and seven theft of trade secrets cases with a nexus to the PRC. We also have brought 12 matters involving fraud on universities and/or grant making institutions.
- There have been four convictions/pleas in the economic espionage/theft of trade secret matters, and four in academic fraud cases.

- We do not track the number of these sorts of cases that we decline or close without charges.

FBI Director Wray said last year that agents are opening a new counterintelligence case related to China every 10 hours and that about half of the FBI's nearly 5,000 investigations related to China. Is that still the case? If not, can you update those numbers?

- How the FBI defines an investigation, which can be a purely intelligence investigation, is not the same as how DOJ defines an active grand jury investigation. We do not disclose the latter number.

Thanks!
Ellen and David

From: Nakamura, David <(b) (6)
Sent: Friday, August 20, 2021 6:15 PM
To: Hornbuckle, Wyn (PAO) <(b) (6) Nakashima, Ellen <(b) (6)
Subject: RE: China initiative interview

Hi Wyn,

Thanks for this information. I don't see the Lu/Liu case included on DOJ's list of China Initiative case examples here https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (I did see the separate press release the department issued here https://www.justice.gov/usao-wdok/pr/husband-and-wife-working-university-arrested-wire-fraud-involving-department-energy)

- As to the Lu/Liu case, the original indictment charged them with straightforward fraud, stemming from their using university and grant money for personal expenses. Although charges were later added in a superseding indictment, they ultimately agreed to plead guilty to the original fraud conduct, so the case was not included on the list.

But some other cases are not listed on that first list of more than 70 cases, including the charges against MIT professor Gang Chen and the Qing Wang case, which advocates who track the initiative said was removed from the list after the case was dropped. Can you please help us understand what this list is: https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related Is it supposed to be an exhaustive list of China Initiative cases or just representative samples? And why is the Gang Chen case not included? How many China-related cases since Nov. 2018 are not included on that list?

- It's intended to be a comprehensive list of cases that implicate PRC government policies and practices, but it is compiled by humans so subject to some degree of error. The case against Gang Chen is a simple oversight on our part, and will be added. Also, re Hao Zhang, we included cases that remained pending on or after the announcement of the initiative. We have long been enforcing laws against economic espionage, computer hacking, proliferation, etc., and we apply the same standard (in terms of proof) in deciding to charge cases before and after the initiative was announced.

If it's the latter, how are you deciding which cases to include and why would DOJ take down the Qing Wang case after the charges were dropped?

- The Qing Wang case was removed after the case was dismissed. When a case is dismissed, we refrain from touting or publicizing the allegations.

One other question: The Hao Zhang case appears to have begun in 2015 when he was indicted. He was found guilty by a judge and sentenced in 2020. You are including that in cases brought after 2018 – just for our understanding, could you explain why? See above

Thank you,
Dave

David Nakamura
Washington Post Staff Writer
(b) (6)
o. (b) (6)
c. (b) (6)
Twitter: @davidnakamura

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Friday, August 20, 2021 5:46 PM
To: Nakamura, David <(b) (6) Nakashima, Ellen <(b) (6)

Subject: RE: China initiative interview

Duplicative Material, Document ID: 0.7.1536.72835, Bates Number 22cv02001_22-00878_000040

From: Bratt, Jay (NSD)
Subject: RE: China initiative interview
To: Hickey, Adam (NSD); Hornbuckle, Wyn (PAO)
Sent: August 22, 2021 10:56 PM (UTC-04:00)

Apologies for the vey belated response. As to the Lu/Liu case, the original indictment charged them with straightforward fraud, stemming from their using university and grant money for personal expenses. That sort of conduct did not implicate any national security concerns. The office later, with our approval, added a couple of fraud counts related to their failure to disclose conflicts of interest arising from work and funding in China. However, soon afterwards, they agreed to plead guilty to the original fraud conduct. (b) (5) [redacted].

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Saturday, August 21, 2021 10:03 AM
To: Hornbuckle, Wyn (PAO) <(b) (6) [redacted]
Cc: Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
Subject: Re: China initiative interview

+Jay. We can get you point by point answers but we've never said they are only the cases investigated after 2018.

Adam S. Hickey | National Security Division | (b)(6), (b)(7)(C) per NSD

> On Aug 20, 2021, at 6:45 PM, Hornbuckle, Wyn (PAO) <(b) (6) [redacted] wrote:
>
> Adam – David Nakamura asked about the list of cases last updated in June. Should the Lu/Lui case be listed under the China Initiative? Gang Chen?
>
> I think the answer to why Qing Wang case was removed is obvious, the case was dropped.
>
> As to whether the list is considered exhaustive, I would say it is intended to capture the full scope of cases under the initiative but may be in need of updating from time to time.
>
> Start email from David Nakamura:
>
> I don't see the Lu/Liu case included on DOJ's list of China Initiative case examples here https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (I did see the separate press release the department issued here https://www.justice.gov/usao-wdok/pr/husband-and-wife-working-university-arrested-wire-fraud-involving-department-energy)
>
> But some other cases are not listed on that first list of more than 70 cases, including the charges against MIT professor Gang Chen and the Qing Wang case, which advocates who track the initiative said was removed from the list after the case was dropped. Can you please help us understand what this list is: https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related Is it supposed to be an exhaustive list of China Initiative cases or just representative samples? If it's the latter, how are you deciding which cases to include and why would DOJ take down the Qing Wang case after the charges were dropped? And why is the Gang Chen case not included? How many China-related cases since Nov. 2018 are not included on that list?
>
> One other question: The Hao Zhang case appears to have begun in 2015 when he was indicted. He was found guilty by a judge and sentenced in 2020. You are including that in cases brought after 2018 – just

for our understanding, could you explain why?

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Friday, August 20, 2021 6:00 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Subject: Re: China initiative interview

You'd have to ask CRM on that one. Not aware of any.

It's (b) (5) . Will send.

Adam S. Hickey | National Security Division | (b)(6), (b)(7)(C) per NSD

> On Aug 20, 2021, at 5:32 PM, Hornbuckle, Wyn (PAO) <(b) (6) wrote:
>
> Adam – (b) (5) Also, (b) (5) ?
>
> ---
>
> **From:** Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
> **Sent:** Thursday, August 19, 2021 5:00 PM
> **To:** Newman, David A. (ODAG) <(b) (6) Hornbuckle, Wyn (PAO) <(b) (6) Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
> **Cc:** (b)(6), (b)(7)(C) per NSD ; Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
> **Subject:** RE: China initiative interview
>
> Makes good sense to me.
>
> In addition to the on the record points, I would note that (b) (5) .
>
> ---
>
> **From:** Newman, David A. (ODAG) <(b) (6)
> **Sent:** Thursday, August 19, 2021 4:56 PM
> **To:** Hornbuckle, Wyn (PAO) <(b) (6) Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >; Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >
> **Cc:** (b)(6), (b)(7)(C) per NSD Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
> **Subject:** RE: China initiative interview
>
> This looks good to me. (I focused in particular on the on-the-record points.) I wonder if we should add an on-the-record point along the following lines (addition in red):
>
> **CHINA INTIATIVE TOP LINE MESSAGES AND BACKGROUND**

DOJ spokesperson:

- (b) (5) [redacted]
- (b) (5) [redacted]
- (b) (5) [redacted]
- (b) (5) [redacted]

From: Hornbuckle, Wyn (PAO) <(b) (6) [redacted]
Sent: Thursday, August 19, 2021 3:45 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; Newman, David A. (ODAG) <(b) (6) [redacted]
Cc: (b)(6), (b)(7)(C) per NSD [redacted] Coley, Anthony D. (PAO) <(b) (6) [redacted] Shevlin, Shannon (PAO) <(b) (6) [redacted]
Subject: RE: China initiative interview

Attached is a cleaned up version with Adam's comment reinserted. Let me know what would work well for your tomorrow.

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >
Sent: Thursday, August 19, 2021 1:53 PM
To: Hornbuckle, Wyn (PAO) <(b) (6) [redacted] Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; Newman, David A. (ODAG) <(b) (6) [redacted]
Cc: (b)(6), (b)(7)(C) per NSD [redacted] Coley, Anthony D. (PAO) <(b) (6) [redacted] Shevlin, Shannon (PAO) <(b) (6) [redacted]
Subject: RE: China initiative interview

Thanks, Wyn. I'm comfortable with this (and tomorrow is a good day to do something by phone). I would (b) (5) [redacted]

(b) (5)
.

Adam

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Thursday, August 19, 2021 1:38 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >; Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD ; Newman, David A. (ODAG) <(b) (6)
Cc: (b)(6), (b)(7)(C) per NSD v>; Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
Subject: RE: China initiative interview

I accepted most of the changes, cut back a bit, and reordered this document as a Spokesperson statement, and background from a DOJ official.

In terms of strategy, I still believe (b) (5)

There is also an LA Times inquiry along these same lines.

Thoughts? (b) (5) ?

Wyn Hornbuckle
Deputy Director, Office of Public Affairs
U.S. Department of Justice
O: (b) (5)
M: (b) (5)

From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >
Sent: Thursday, August 19, 2021 9:37 AM
To: Hornbuckle, Wyn (PAO) <(b) (6) Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; Newman, David A. (ODAG) <(b) (6)
Cc: (b)(6), (b)(7)(C) per NSD Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
Subject: RE: China initiative interview

Thanks, Wyn, for taking the lead on drafting. Attached are Jay and my edits to this. I think (b) (5)
.

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Thursday, August 19, 2021 9:23 AM
To: Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD >; Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >; Newman, David A. (ODAG) <(b) (6)
Cc: (b)(6), (b)(7)(C) per NSD Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)

Subject: RE: China initiative interview

Thanks Jay. This filing is a perfect counter to the assertion that NIH sources don't see this as a law enforcement problem. Zheng received 37 months in prison. https://www.justice.gov/opa/pr/university-researcher-sentenced-prison-lying-grant-applications-develop-scientific-expertise

Attached are DRAFT top line messages and more specific questions we can expect (based on my conversation with both David Nakamura and Ellen Nakashima). I still believe (b) (5)

Unfortunately, the lead in the WaPo story will be the wire fraud case dropped by SDOH against Dr. Qing Wang, a former Cleveland Clinic Foundation employee, charged with false claims and wire fraud related to more than $3.6 million in grant funding that Dr. Wang and his research group received from the National Institutes of Health (NIH). Former Cleveland Clinic Employee and Chinese "Thousand Talents" Participant Arrested for Wire Fraud | OPA | Department of Justice .
They will press DOJ on why these were charged and why this case is no longer included int the China initiative cases? (b) (5)
)

Are folks available to circle up on a call later today? I am free until 12, then 1 – 2, and 2:30 – 5 p.m.

Or otherwise feel free to dive in and make edits to the document.

Wyn Hornbuckle
Deputy Director, Office of Public Affairs
U.S. Department of Justice
O:(b) (5)
M:(b) (5)

From: Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Tuesday, August 17, 2021 4:51 PM
To: Hornbuckle, Wyn (PAO) <(b) (6) Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Newman, David A. (ODAG) <(b) (6)
Cc: (b)(6), (b)(7)(C) per NSD Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
Subject: RE: China initiative interview

Attached is the Lauer Declaration that I mentioned during the call.

From: Hornbuckle, Wyn (PAO) <(b) (6)
Sent: Tuesday, August 17, 2021 4:45 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD Newman, David A. (ODAG) <(b) (6) Bratt, Jay (NSD) (b)(6), (b)(7)(C) per NSD
Cc: (b)(6), (b)(7)(C) per NSD Coley, Anthony D. (PAO) <(b) (6) Shevlin, Shannon (PAO) <(b) (6)
Subject: RE: China initiative interview

Attached are some draft talking points, and a series of Questions based on my conversation this afternoon with both Ellen Nakashima and David Nakamura. They will give you a clear idea of the direction the article is going, likely to publish next week. Let's circle up tomorrow to discuss when folks have a chance to digest this.

-----Original Appointment-----
From: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Monday, August 16, 2021 2:41 PM
To: Hickey, Adam (NSD); Newman, David A. (ODAG); Bratt, Jay (NSD)
Cc: Hornbuckle, Wyn (PAO); (b)(6), (b)(7)(C) per NSD (NSD); Coley, Anthony D. (PAO); Shevlin, Shannon (PAO)
Subject: China initiative interview
When: Tuesday, August 17, 2021 11:30 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting (or NSD OAAG)

Join Microsoft Teams Meeting

(b) (6) United States, Washington (Toll)

Conference ID: (b) (6)

Local numbers | Reset PIN | Learn more about Teams

From: Newman, David A. (ODAG) <(b) (6)
Sent: Monday, August 16, 2021 2:35 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD>
Cc: Hornbuckle, Wyn (PAO) <(b) (6) (b)(6), (b)(7)(C) per NSD
Subject: Re: China initiative interview

Tomorrow at 11:30am is good here.

> On Aug 16, 2021, at 2:33 PM, Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD> wrote:
>
> I'm free until 330 pm. Otherwise, tomorrow works at 11:30 am.
>
> **From:** Hornbuckle, Wyn (PAO) <(b) (6)
> **Sent:** Monday, August 16, 2021 2:31 PM
> **To:** Newman, David A. (ODAG) <(b) (6)
> **Cc:** (b)(6), (b)(7)(C) per NSD Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
> **Subject:** RE: China initiative interview

Ellen would like to do an interview on Thursday on this. Can we have a call internally this afternoon or tomorrow morning sometime to discuss? I'm free today until 4, then after 5:30, or tomorrow around 10:30 or 11:30

From: Newman, David A. (ODAG) <(b) (6)
Sent: Friday, August 13, 2021 5:03 PM
To: Hornbuckle, Wyn (PAO) <(b) (6)
Cc: (b)(6), (b)(7)(C) per NSD Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Subject: Re: China initiative interview

Sounds good. And this dovetails with discussions we've been having ((b)(6), (b)(7)(C) per NSD Adam, and I) over the past few weeks.

> On Aug 13, 2021, at 5:00 PM, Hornbuckle, Wyn (PAO) <(b) (6) wrote:
>
> Thanks David. Happy to circle up on Monday, maybe sometime in the afternoon we could have a quick call
>
> ---
>
> **From:** Newman, David A. (ODAG) <(b) (6)
> **Sent:** Friday, August 13, 2021 3:35 PM
> **To:** Hornbuckle, Wyn (PAO) <(b) (6)
> **Cc:** (b)(6), (b)(7)(C) per NSD Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
> **Subject:** Re: China initiative interview
>
> Thank you. Happy to confirm with NSD about this on Monday and circle back.
>
> > On Aug 13, 2021, at 2:44 PM, Hornbuckle, Wyn (PAO) <(b) (6) wrote:
> >
> > I spoke to Ellen, and I was incorrect that they were asking the Associate's office about this, but Nakamura is digging into the civil rights angle. Ellen also asked about the role of grant making organizations, like NIH or NASA, and whether prosecution is the right mechanism for dealing with this given some of the challenges that some of the cases have seen (PLA researchers, Hu case, etc)
> >
> > Also adding ODAG, as this will also runs to the heart of where the Initiative goes from here, what have we learned, what worked and must continue etc.
> >
> > ---
> >
> > **From:** Hornbuckle, Wyn (PAO)
> > **Sent:** Friday, August 13, 2021 2:20 PM
> > **To:** (b)(6), (b)(7)(C) per NSD Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD

Subject: FW: China initiative interview

Let me know your thoughts about this. I am thinking (b) (5) .
They are also pinging the Associate's office on the CRT angle, so will need to coordinate with them on this. The statement I started working on the other week may come in handy here as an official response.

From: Nakashima, Ellen
(b) (6)
Sent: Friday, August 13, 2021 1:29 PM
To: Hornbuckle, Wyn (PAO)
(b) (6)
Cc: Nakamura, David
(b) (6)
Subject: China initiative interview

Hi, Wyn –

I mentioned to you that we'd be coming back to you on the China initiative. David Nakamura, who covers the civil rights division, is working on a piece with me examining the impact of the China initiative on the U.S. academic community in the broader context of the overall goal and outcomes of the initiative.

What exactly, is the goal of the initiative? Is it primarily, as has been suggested, to deter Chinese economic espionage (and trade secret theft)? Is it broader?

How many cases have been brought under the program since Nov. 2018, and how many have resulted in convictions –on what charges? How many have been concluded without charges? How many involve defendants who are academics and scientific researchers? How many investigations are ongoing?

We have gathered numbers as best we can but would like to know what your statistics are.

We have a number of other questions but wanted to give you a general sense of what we're interested in. And we'd like to hear your perspective on the effectiveness of the program three years in.

Can we arrange something for Monday morning?

Bests,
Ellen

From: (b)(6) Marc Raimondi (PAO)
Subject: Re: Wei Sun/Raytheon sentencing question
To: Reenat Sinay
Sent: November 18, 2020 1:58 PM (UTC-05:00)

We do not limit the China initiative to any specific charge so yes, you can put this under the China initiative umbrella.

Marc Raimondi
U.S. Department of Justice
(b) (6)

On Nov 18, 2020, at 1:37 PM, Reenat Sinay <(b) (6) wrote:

Hi Marc,

I'm writing about the sentencing announced today and was wondering if this enforcement effort is considered to be part of the DOJ's wider China Initiative? The press release doesn't specifically say so and Sun wasn't charged with trade secret theft or espionage, so I just wanted to clarify. My deadline is 3:30pm ET.

Thanks,

--
Reenat Sinay
Reporter

Legal News & Data
111 W. 19th Street, 5th Floor
New York, NY 10011
(b) (6)

From: Creegan, Erin (ODAG)
Subject: FW: DRAFT DOJ Press Release - China Initiative Year-in-Review 2019-20 v. 2020 10 30 1615
To: Newman, Ryan D. (OAG)
Sent: November 2, 2020 12:29 PM (UTC-05:00)
Attached: DRAFT DOJ Press Release - China Initiative Year-in-Review 2019-20 v. 2020 10 30 1845.docx

DAG wanted to check if AG wants to comment?

From: Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Sunday, November 1, 2020 3:29 PM
To: Creegan, Erin (ODAG) <(b) (6) Raimondi, Marc (OPA) <(b) (6)
Subject: Fwd: DRAFT DOJ Press Release - China Initiative Year-in-Review 2019-20 v. 2020 10 30 1615

Erin and Marc,

Attached is a proposed press release on the two year anniversary of the China Initiative, covering this past year's highlights.

Marc, (b) (5) .

Up to you guys on timing. Today is the two year anniversary but I think any time in early November works.

John

From: Raimondi, Marc (OPA)
Subject: FW: Week Ahead for Sept. 28th
To: John C. Demers (b)(6), (b)(7)(C) per NSD; David Burns (NSD) (b)(6), (b)(7)(C) per NSD; [redacted] (NSD); (b)(6), (b)(7)(C) per NSD ; Hickey, Adam (NSD)
Sent: September 28, 2020 12:22 PM (UTC-04:00)

Any thoughts on if we should wrap up these types of cases when they have a NEXUS to china under the China Initiative? It is not economic espionage but can be the back side of EE and trade secret theft.

Just a thought.

- On September 29, Lin Dong, a New York businessman, will be sentenced for his role in Operation TMG. Over the course of the scheme, the conspirators attempted to import counterfeit goods with a total estimated Manufacturer's Suggested Retail Price, had they been genuine, of over $1,000,000,000. The defendant was a wholesale trafficker of the counterfeit luxury goods. He is the third defendant to be sentenced out of 17 who have pleaded guilty federally. The guilty defendants have agreed to forfeit over $4,700,000 in criminal proceeds. Eleven additional defendants have pleaded guilty in New York state cases based on the investigation.

FOR IMMEDIATE RELEASE
Thursday, August 16, 2018

22 Charged with Smuggling Millions of Dollars of Counterfeit Luxury Goods from China into The United States

Defendants Trafficked Items that Included Fake Louis Vuitton and Tory Burch Handbags, Michael Kors Wallets, Hermes Belts and Chanel Perfume

Earlier today, in federal court in Brooklyn, six indictments and one criminal complaint were unsealed charging a total of 22 defendants with illegally bringing into the United States millions of dollars of Chinese-manufactured goods by smuggling them through ports of entry on the East and West Coasts. The defendants were arrested this morning, and their initial appearances and arraignments are scheduled this afternoon before United States Magistrate Judge Lois Bloom.

The charges include conspiracy to traffic, and trafficking, in counterfeit goods; conspiracy to smuggle, and smuggling, counterfeit goods into the United States; money laundering conspiracy; immigration fraud and unlawful procurement of naturalization. In addition, the government restrained nine real properties in Queens, Staten Island and Brooklyn, New York, belonging to the defendants.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, Brian A. Benczkowski, Assistant Attorney General for the U.S. Department of Justice's Criminal Division, Angel M. Melendez, Special Agent-in-Charge, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), New York, and James P. O'Neill, Commissioner, New York City Police Department (NYPD), announced the charges.

"As alleged, the defendants used many forms of deception to smuggle large quantities of counterfeit luxury brand goods from China into the United States, and then profited by distributing and selling the fake merchandise," stated United States Attorney Donoghue. "This Office, working with our law enforcement partners, is committed to securing our country's ports of entry, as well as to protecting the integrity of intellectual property upon which free and fair international trade and markets depend." Mr. Donoghue extended his grateful appreciation to the HSI Intellectual Property Group and the HSI Border Enforcement Security Task Force and the NYPD. Mr. Donoghue also extended his thanks to U.S. Customs and Border Protection, the New York State Police and the Brooklyn District Attorney's Office for their assistance.

"The defendants allegedly smuggled millions of dollars of counterfeit luxury goods into our country, depriving companies of their valuable and hard-earned intellectual property," stated Assistant Attorney General

Benczkowski. "The illegal smuggling of counterfeit goods poses a real threat to honest businesses, and I commend our federal prosecutors and partners at HSI and the NYPD for their outstanding work on this important investigation. The Department of Justice is committed to holding accountable those who seek to exploit our borders by smuggling counterfeit goods for sale on the black market."

"This investigation exposed the global nature of intellectual property crimes, allegedly being executed by those arrested today. Counterfeit goods manufactured and smuggled from China with a suggested value north of half a billion dollars, were intended to make its way into U.S. markets and into the hands of unsuspecting consumers," said HSI Special Agent-in-Charge Melendez. "This investigation should be a crystal clear message that counterfeiting and intellectual property rights violations is anything but a victimless crime as it harms legitimate businesses, consumers and governments."

"Today's indictments demonstrate our resolve to ensure a level playing field for all, and serve as a reminder that selling fake goods is never a victimless crime," stated NYPD Commissioner O'Neill. "Everything about these activities undermines public trust. And the NYPD, in close collaboration with all of our local, state, and federal law enforcement partners, will continue to aggressively combat and prosecute the evasive practices of the individuals and companies who attempt to operate outside our laws and regulations."

According to the court filings, the defendants played various roles in the trafficking of counterfeit goods manufactured in China, brought by ocean-going ships to the United States in 40-foot shipping containers, smuggled through ports of entry disguised as legitimate imports and distributed throughout the country. The counterfeit goods included items such as fake Louis Vuitton and Tory Burch handbags, Michael Kors wallets, Hermes belts and Chanel perfume. The defendants' roles included:

Importers

Qi Feng Liang, Wo Qi Liu, Zhi Ming Zhang and Yu Ming Wong served as shipping container importers. They arranged to smuggle counterfeit goods into the United States through the Port of New York/New Jersey and elsewhere. They fraudulently used the names, addresses and other identifying information of legitimate import companies and falsified the descriptions of the containers' contents on U.S. customs paperwork associated with the containers of counterfeit goods. They used "burner" phone numbers and "burner" email accounts—obtained by using false or incomplete information—in order to conceal their true identities. The counterfeit goods were transported by trucks to self-storage facilities in Brooklyn, Queens and Long Island, New York, where the goods were unloaded and stored. Qi Feng Liang, Wo Qi Liu, Zhi Ming Zhang and Yu Ming Wong smuggled or attempted to smuggle 23 40-foot shipping containers into the country loaded with counterfeit items. The estimated Manufacturers' Suggested Retail Price of these items, had they been genuine, would have been more than $450 million.

Wholesale Distributors

Josstina Lin, Xue Wei Qu, Xi Quan Huang, Yun Lei Huang, Yun Wu Huang, Si Lung Chung, Le Wei Zheng, Xiao Ying Huang, Qiong Chan Mu, Ren Zhong Zhu, Cheng Xu Yu, Jin Hua Zhang, Jian Hua Zhu, Yong Lin Dong and Cai Ying Lin managed the receipt, storage and distribution of counterfeit goods smuggled into the United States by the importers. They resold the counterfeit items to other wholesale and retail sellers in New York, California and elsewhere in the United States.

Domestic Shippers

Wei Mei Gao, Sheng Miao Xia and Jie Mei Chen used private shipping businesses they controlled to distribute the counterfeit goods smuggled into the United States by the importers and handled by the wholesale distributors. The domestic shippers also facilitated payments by the wholesale and retail counterfeit goods sellers to the wholesale distributors.

As alleged in the indictments, some defendants additionally conspired to launder the proceeds from the sale of counterfeit goods, and others illegally concealed their involvement in the trafficking of counterfeit goods when applying for immigration benefits.

The charges in the indictments and criminal complaint are allegations, and the defendants are presumed innocent unless and until proven guilty.

The government's cases are being prosecuted by Assistant United States Attorneys William P. Campos and Temidayo Aganga-Williams of the Eastern District of New York, Special Assistant United States Attorney Robert Kaftal of the Brooklyn District Attorney's Office and Senior Counsel James S. Yoon of the U.S. Department of Justice, Criminal Division Computer Crime and Intellectual Property Section (CCIPS). Assistant United States Attorney Claire S. Kedeshian is handling the forfeiture aspect of this case. The investigation was previously led by Senior Counsel Evan Williams of CCIPS.

The Department of Justice's Task Force on Intellectual Property (IP Task Force) contributed to this case. The IP Task Force is led by the Deputy Attorney General to combat the growing number of domestic and intellectual property crimes, to protect the health and safety of American consumers and to safeguard the nation's economic security against those who seek to profit illegally from American creativity, innovation and hard work. To learn more about the IP Task Force, go to https://www.justice.gov/iptf. For more information about the U.S. Attorney's Office for the Eastern District of New York, visit its website at https://www.justice.gov/usao-edny.

- **The Defendants:**

- QI FENG LIANG (also known as "Alex" and "Mike Sotire")
  Age: 34
  Brooklyn, New York

- WO QI LIU (also known as "Louis," "Qi," "Woqi" and "Big Elephant")
  Age: 43
  Brooklyn, New York

- ZHI MING ZHANG (also known as "Jordan" and "Four B")
  Age: 43
  Staten Island, New York

- JOSSTINA LIN (also known as "Tina")
  Age: 42
  Brooklyn, New York

- XUE WEI QU
  Age: 51
  Queens, New York

- E.D.N.Y. Docket No. 18-CR-419 (WFK)

- XI QUAN HUANG
  Age: 58
  Queens, New York

- YUN LEI HUANG
  Age: 32
  Queens, New York

- YUN WU HUANG
  Age: 34
  Queens, New York

- WEI MEI GAO
  Age: 35
  Queens, New York

- SHENG MIAO XIA
  Age: 44
  Queens, New York

- E.D.N.Y. Docket No. 18-CR-408

- SI LUNG CHUNG (also known as “Allan”)
  Age: 42
  New York, New York

- LE WEI ZHENG
  Age: 42
  New York, New York

- E.D.N.Y. Docket No. 18-CR-407 (CBA)

- XIAO YING HUANG (also known as “Linda”)
  Age: 53
  Nassau County, New York

- QIONG CHAN MU (also known as “Rosanna”)
  Age: 26
  Nassau County, New York

- REN ZHONG ZHU
  Age: 31
  Nassau County, New York

- E.D.N.Y. Docket No. 18-CR-423 (DLI)

- YONG LIN DONG
  Age: 43
  Queens, New York

- CAI YING LIN
  Age: 43
  Queens, New York

- CHENG XU YU (also known as “Vic”)
  Age: 29
  Queens, New York

- JIAN HUA ZHU
  Age: 52
  Queens, New York

- JIN HUA ZHANG
  Age: 55
  Queens, New York

- E.D.N.Y. Docket No. 18-CR-396 (JBW)

- JIE MEI CHEN (also known as “Jenny”)
  Age: 33
  Queens, New York

- E.D.N.Y. Docket No. 18-CR-409 (BMC)

- YU MING WONG
  Age: 36
  Queens, New York

- E.D.N.Y. Docket No. 18-MJ-752

From: Timmons, Mollie R. (PAO) <(b) (6)
Sent: Friday, September 25, 2020 1:00 PM
To: Lloyd, Matt (PAO) <(b) (6)
Cc: Nichols, Danielle (PAO) <(b) (6) Kjergaard, Alison (OPA) <(b) (6) Navas, Nicole (OPA) <(b) (6) McGowan, Ashley L. (OPA) <(b) (6) Creighton, Kelly M (OPA) <(b) (6) Raimondi, Marc (OPA) <(b) (6) Lloyd, Matt (PAO) <(b) (6) Mastropasqua, Kristina (OPA) <(b) (6) Flynn, Mell (OPA) <(b) (6) Fauntleroy, Priscilla M. (OPA) <(b) (6) Queen, Auriahn (OPA) <(b) (6) Clark, Melissa D. (PAO) <(b) (6) Cardwell, Jeff (PAO) <(b) (6) Herlihy, Brianna (PAO) <(b) (6) Vance, Alexa M. (PAO) <(b) (6) Kupec, Kerri (OPA) <(b) (6) Morales, Arlen M. (PAO) <(b) (6)
Subject: Week Ahead for Sept. 28th

Week Ahead

September 28th – October 2nd

Monday, September 28th

USAO

- USAO SDFL, DEA, and INL will announce narcotics rewards for three former Venezuelan Officials: $10 million for information leading to the arrest and/or conviction of Pedro Luis Martin-Olivares, the former Chief of Economic Intelligence, and up to $5 million each for information leading to the arrests and/or convictions of Rodolfo McTurk-Mora, the former head of Interpol in Venezuela, and Jesus Alfredo Itriago, the former Chief of Counternarcotics for the Cuerpo de Investigaciones Científicas, Penales y Criminálisticas (CICPC). Martin-Olivares, indicted on April 24, 2015 in SDFL for narcotics trafficking related crimes. (b) (5) . LES

CRM

- On September 28, Jimmy Villalobos-Gomez and Walter Antonio Chicas-Garcia will be indicted for VICAR murder (b) (5) . LES
- (b) (5)

ENRD

- The U.S. Environmental Protection Agency (EPA) and the Department of Justice will announce a settlement with the Churchill Downs Louisiana Horseracing Company, LLC, d/b/a Fair Grounds Corporation (Fair Grounds) that will resolve years of Clean Water Act (CWA) violations at its New Orleans racetrack. Under the settlement, Fair Grounds will eliminate unauthorized discharges of manure, urine and process wastewater through operational changes and construction projects at an estimated cost of $5,600,000. The company also will pay a civil penalty of $2,790,000, the largest ever paid by a concentrated animal feeding operation in a CWA matter.

OJP

- DOJ podcast on Operation Lady Justice will be live. Wyn interviewed Katie Sullivan for the podcast.

Tuesday, September 29th

CRM

- On September 29, Andrew "Dale" Ledbetter, an attorney, will be charged with one count of conspiracy to commit securities fraud and wire fraud by information in relation to an investment fraud scheme at 1 Global Capital (1GC), based in Hallandale Beach, Florida. (b) (5) The fraud involved false representations to investors concerning the profitability of the business, the use and diversion of investor funds, and the applicability of the federal securities laws to the investment offering. The charges stem from Ledbetter's role as the primary marketing representative and investor relations spokesperson. Among other misrepresentations, Ledbetter falsely claimed that 1GC's offering was not a security; used false opinion letters authored by a co-conspirator to justify the continued marketing and sale of 1 Global's offering, despite mounting concerns regarding its status as a security; falsely claimed that 1 Global's financials were audited by an outside accounting firm; and concealed the degree to which he personally received commissions based upon the volume of new investments. LES

- On September 29, Lin Dong, a New York businessman, will be sentenced for his role in Operation TMG. Over the course of the scheme, the conspirators attempted to import counterfeit goods with a total estimated Manufacturer's Suggested Retail Price, had they been genuine, of over $1,000,000,000. The defendant was a wholesale trafficker of the counterfeit luxury goods. He is the third defendant to be sentenced out of 17 who have pleaded guilty federally. The guilty defendants have agreed to forfeit over $4,700,000 in criminal proceeds. Eleven additional defendants have pleaded guilty in New York state cases based on the investigation.

Wednesday, September 30th

CRM

- Health Care Fraud press conference at 11 a.m. with FBI, DEA, and HHS
- (b) (5) LES
- (b) (5)

Thursday, October 1st

CRM

- (b) (5)

(b) (5)

LES

- (b) (5)
- (b)(6), (b)(7)(A), (b)(7)(C) per CRM

Friday, October 2nd

CRM

- On October 2, Roberto Heinert will plead guilty to one count of conspiracy to commit money laundering

(b) (5)

Next Week – TBD

AG

- Scheduled for Tuesday and Wednesday – travel to St. Louis, Missouri and Tulsa, Oklahoma

From: Burns, David P. (NSD)
Subject: RE: PRC Economic Espionage
To: Hamilton, Gene (OAG); Blue, Matthew (ODAG); Creegan, Erin (ODAG); Mascott, Jenn (ODAG); Hodes, Jarad (ODAG)
Cc: Sofer, Gregg (OAG); Newman, Ryan D. (OAG); (b)(6), (b)(7)(C) per NSD (NSD)
Sent: August 14, 2020 2:35 PM (UTC-04:00)

Correct.

David P. Burns
Principal Deputy Assistant Attorney General
National Security Division
U.S. Department of Justice
(b)(6), (b)(7)(C) per NSD

-----Original Message-----
From: Hamilton, Gene (OAG) (b) (6)
Sent: Friday, August 14, 2020 1:56 PM
To: Burns, David P. (NSD) (b)(6), (b)(7)(C) per NSD ; Blue, Matthew (ODAG) (b) (6)
Creegan, Erin (ODAG) (b) (6) ; Mascott, Jenn (ODAG)
(b) (6) ; Hodes, Jarad (ODAG) (b) (6)
Cc: Sofer, Gregg (OAG) (b) (6) Newman, Ryan D. (OAG)
(b) (6) ; (b)(6), (b)(7)(C) per NSD
Subject: RE: PRC Economic Espionage

Thank you, David. No issue with me sharing this list with DHS, correct?

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

-----Original Message-----
From: Burns, David P. (NSD) (b)(6), (b)(7)(C) per NSD
Sent: Friday, August 14, 2020 1:37 PM
To: Blue, Matthew (ODAG) (b) (6) ; Hamilton, Gene (OAG)
(b) (6) ; Creegan, Erin (ODAG) (b) (6) ; Mascott, Jenn
(ODAG) (b) (6) ; Hodes, Jarad (ODAG) (b) (6)
Cc: Sofer, Gregg (OAG) (b) (6) ; Newman, Ryan D. (OAG)
(b) (6) ; (b)(6), (b)(7)(C) per NSD
Subject: RE: PRC Economic Espionage

Attached is a list of our charged economic espionage cases involving private industry that are part of our China Initiative. I am also copying my colleague (b)(6), (b)(7)(C) per NSD, who prepared the summary, in case there are questions.

David P. Burns
Principal Deputy Assistant Attorney General National Security Division U.S. Department of Justice
(b)(6), (b)(7)(C) per NSD

-----Original Message-----
From: Blue, Matthew (ODAG) (b) (6)
Sent: Thursday, August 13, 2020 12:47 PM

To: Hamilton, Gene (OAG) (b) (6) >; Creegan, Erin (ODAG) (b) (6) ; Mascott, Jenn (ODAG) (b) (6) ; Hodes, Jarad (ODAG) (b) (6)
Cc: Sofer, Gregg (OAG) (b) (6) ; Newman, Ryan D. (OAG) (b) (6) ; Burns, David P. (NSD) (b)(6), (b)(7)(C) per NSD
Subject: RE: PRC Economic Espionage

Gene,

Good afternoon and I hope all is well with you. Adding David Burns for help on that question.

Best,

Matt

Matthew F. Blue

Associate Deputy Attorney General

U.S. Department of Justice

(b) (6)

From: Hamilton, Gene (OAG) (b) (6)
Sent: Thursday, August 13, 2020 11:50 AM
To: Blue, Matthew (ODAG) (b) (6) ; Creegan, Erin (ODAG) (b) (6) ; Mascott, Jenn (ODAG) (b) (6) ; Hodes, Jarad (ODAG) (b) (6)
Cc: Sofer, Gregg (OAG) (b) (6) ; Newman, Ryan D. (OAG) (b) (6)
Subject: FW: PRC Economic Espionage

Hey y'all,

Do you know if NSD has maintained a list of these types of cases? If so, would we be able to share it (or any portions thereof) so that they could run the identifying information through it to analyze the underlying immigration status of each individual to identify patterns or any possible improvements in vetting/screening?

Thanks!

Gene P. Hamilton

Counselor to the Attorney General

U.S. Department of Justice

From: (b)(6) per DHS
Sent: Thursday, August 13, 2020 11:34 AM
To: Hamilton, Gene (OAG) (b) (6)
Subject: PRC Economic Espionage

Hi Gene,

I hope you are doing well!

I`m running point on immigration issues for the newly formed DHS China working group.

One of the areas I'm examining are the ways that the PRC uses our visa employment programs to conduct IP and tech theft of U.S companies.

Thus far, I've found the below examples from DOJ. What I can't find are the specific visa statuses for these individuals which provided them entry into the U.S.

Is there a contact within DOJ who I could reach out to on this topic? Additionally, are there further examples that DOJ has of PRC economic espionage occurring at U.S companies?

https://www.justice.gov/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets

https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy

https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets

https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading

Regards,

(b)(6) per DHS

Immigration Policy

U.S. Department of Homeland Security

(b) (6)

FOR OFFICIAL USE ONLY - NOT FOR PUBLIC RELEASE

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
7/21/20	U.S. v. Li and Dong	EDWA	Li Xiaoyu and Dong Jiazhi	1030/consp.; 1832 consp.; 1373; 371; 1028	No	(b)(6) per NSD		biomed; medical; solar; manufacturing; software; defense
2/13/20	U.S. v. Huawei	EDNY	Huawei Technologies Co., Ltd.; Huawei Device Co., Ltd.; Huawei Device USA Inc.; Futurewei Technologies	RICO	No			telecomm
1/28/20	U.S. v. Zhiyong	NDGA	Wu Zhiyong, Wang Qian, Xu Ke, Liu Lei	1831 consp,, 1831; 1832 consp., 1030 (x3); 1030 (x2); 1343 consp.; 1343	Yes			PII; data compilations and database designs

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
11/21/19	U.S. v. Xiang	EDMO	Haitao Xiang	1831 conspiracy, 1831, 1832 conspiracy, 1832	Yes	(b)(6) per NSD		agricultural
9/16/19	U.S. v. Zhou, Chen	SDOH	Yu Zhou and Li Chen	1832 conspiracy, theft; 1343 - conspiracy/wire fraud	No			biopharma
8/14/19	U.S. v. Bo Mao	EDNY	Bo Mao	1343 wire fraud	No			computer storage
6/14/19	U.S. v. Haoyang Yu and Tricon MMIC, LLC	DMA	Haoyang Yu; Tricon MMIC, LLC.	1832 conspiracy/theft; smuggling	No			semiconductor
4/23/19	U.S. v. Xiaoqing Zheng	NDNY	Xiaoqing Zheng	1831 consp/theft; 1832 consp/theft; 1001	Yes			turbines/power
2/12/19	U.S. v. Xiarong You and Liu Xiangchen	EDTN	Xiarong You and Liu Xiangchen	1832 consp./theft; wire fraud	No			BPA-free coatings for food/beverage industry

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
1/31/19	U.S. v. Jizhong Chen	NDCA	Jizhong Chen	1832 theft	No	(b)(6) per NSD		autonomous vehicles
1/28/19	U.S. v. Huawei	WDWA	Huawei Device Co., Ltd.; Huawei Device USA, Inc.	1832 consp./att; wire fraud; obstruction	No			robotics (for cellular phone testing)
1/28/19	U.S. v. Huawei, et al.	EDNY	Huawei Technologies Co., Ltd.; Huawei Device USA Inc.; Skycom Tech Co., Ltd.; Wanzhou Meng	bank fraud & consp.; wire fraud & consp; 371; IEEPA & consp.; money laundering consp.; obstruction consp.	No			N/A
12/20/18	U.S. v. Hongjin Tan	WDOK	Hongjin Tan	1832 theft	No			energy/battery

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
12/20/18	U.S. v. Zhu Hua and Zhang Shilong	SDNY	Zhu Hua and Zhang Shilong	1030 consp.; wire fraud consp.; agg. Identity theft	No	(b)(6) per NSD		aviation, satellite, maritime, automation, automotive, banking an finance, telecomm, consumer electronics, semiconductor, IT, consulting, healthcare, mining, energy, etc.
11/1/18	U.S. v. United Microelectronics, et al.	NDCA	Fujian Jinhua (PRC); United Microelectronics (Taiwan); Stephen Chen; He Jianting; Wang Yungmin	1831 consp./theft; 1832 consp./theft	Yes			DRAM advanced computer memory

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
10/25/18	U.S. v. Zhang Zhang-gui, et al.	SDCA	Zhang Zhang-gui; Zha Rong; Chain Meng; Liu Chunliang; Gao Hong Kun; Zhuang Xiaowei; Ma Zhiqi; Li Xiao; Gu Gen; Tian Xi	1030 consp./sub.	No	(b)(6) per NSD		commercial aviation
10/10/18	U.S. v. Yanjun Xu	SDOH	Yanjun Xu	1831 consp./att; 1832 consp./att	Yes			commercial aviation (fan blades)
7/16/18	U.S. v. Xiaolang Zhang	NDCA	Xiaolang Zhang	1832 theft	No			autonomous vehicles

Date public	Case name	District	Defendants	Charges	EE	U.S. Citizenship	Entry Visa type	Industry, products targeted
4/27/18	U.S. v. Shi, et al.	DDC	Shan Shi, Kui Bo, Gang Liu, Samuel Ogoe, Uka Uche, Hui Huang, Taizhou CBM Future New Material Science and Tech Co., CBM International	1831 consp., 1832 consp., money laundering	Yes	(b)(6) per NSD		Syntactic foam

From: Hamilton, Gene (OAG)
Subject: Fwd: Time Sensitive Request
To: Whitaker, Henry C. (OLC); Hart, Rosemary (OLC)
Sent: May 22, 2020 10:20 PM (UTC-04:00)

Here's one from the list:

https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

Gene P. Hamilton
Counselor to the Attorney General

Begin forwarded message:

From: "Raimondi, Marc (OPA)" (b) (6)
Date: May 22, 2020 at 10:07:59 PM EDT
To: "Hart, Rosemary (OLC)" (b) (6)
Cc: "Demers, John C. (NSD)" (b)(6), (b)(7)(C) per NSD, "Hamilton, Gene (OAG)" (b) (6), (b)(6), (b)(7)(C) per NSD (b)(6), (b)(7)(C) per NSD "Whitaker, Henry C. (OLC)" (b) (6) "Newman, Ryan D. (OAG)" (b) (6), "Blue, Matthew (ODAG)" (b) (6), "Hickey, Adam (NSD)" (b)(6), (b)(7)(C) per NSD
Subject: Re: Time Sensitive Request

Sure. Here is the latest: https://www.justice.gov/opa/page/file/1223496/download

Marc Raimondi
U.S. Department of Justice
(b) (6)

On May 22, 2020, at 10:00 PM, Hart, Rosemary (OLC) (b) (6) wrote:

Thanks. That would be great to have.

Sent from my iPhone

> On May 22, 2020, at 9:52 PM, Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD wrote:
>
> Marc,
>
> Will you send the China initiative case list?
>
> Thanks,
> John

On May 22, 2020, at 8:19 PM, Hamilton, Gene (OAG)
(b) (6) wrote:

Hi Team NSD,

I hope that y'all are well. OLC is working on another product right now for the White House. I know we are, and have been, dealing with a large number of IP theft cases involving Chinese nationals across a variety of fronts—and we can all do google searches to find some of our press releases about them—but are you aware of any specific examples of cases involving graduate students from China (or recent graduate students)? If so, could you please send them to Henry Whitaker and Rosemary Hart? They're on a fairly tight deadline. I don't think we need to reinvent the wheel or anything, but if there are things that are readily available it would be incredibly helpful.

Thank you,

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

From: Masood Farivar
Subject: Re: UNIVERSITY OF KANSAS RESEARCHER INDICTED FOR FRAUD FOR FAILING TO DISCLOSE CONFLICT OF INTEREST WITH CHINESE UNIVERSITY
To: Raimondi, Marc (OPA)
Sent: August 21, 2019 7:05 PM (UTC-04:00)

Got it. Thanks.

From: Raimondi, Marc (OPA) <(b) (6)
Sent: Wednesday, August 21, 2019 7:00 PM
To: Masood Farivar <(b) (6)
Subject: Re: UNIVERSITY OF KANSAS RESEARCHER INDICTED FOR FRAUD FOR FAILING TO DISCLOSE CONFLICT OF INTEREST WITH CHINESE UNIVERSITY

It is certainly China related but it's not charged as economic espionage or as a trade secret theft.

Marc Raimondi
National Security Division
U.S. Department of Justice
(b) (6)
Mobile (b) (6)
Sent from an iPhone, pls excuse shrthnd, typo$ and errant auto-connects.

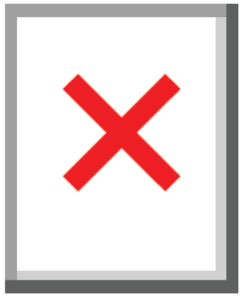
On Aug 21, 2019, at 6:48 PM, Masood Farivar <(b) (6) wrote:

Marc,

Would you put this in the "China Initiative" basket?

Masood

From: USDOJ-Office of Public Affairs <USDOJ-OfficeofPublicAffairs@public.govdelivery.com>
Sent: Wednesday, August 21, 2019 5:23 PM
To: Masood Farivar <(b) (6)
Subject: UNIVERSITY OF KANSAS RESEARCHER INDICTED FOR FRAUD FOR FAILING TO DISCLOSE CONFLICT OF INTEREST WITH CHINESE UNIVERSITY



The United States Department of Justice

UNIVERSITY OF KANSAS RESEARCHER INDICTED FOR FRAUD FOR FAILING TO DISCLOSE CONFLICT OF INTEREST WITH CHINESE UNIVERSITY

WASHINGTON – A researcher at the University of Kansas (KU) was indicted today on federal charges of hiding the fact he was working full time for a Chinese university while doing research at KU funded by the U.S. government.

Feng "Franklin" Tao, 47, of Lawrence, Kansas, an associate professor at KU's Center for Environmentally Beneficial Catalysis (CEBC), is charged with one count of wire fraud and three counts of program fraud. He was employed since August 2014 by the CEBC, whose mission is to conduct research on sustainable technology to conserve natural resources and energy.

"Tao is alleged to have defrauded the U.S. government by unlawfully receiving federal grant money at the same time that he was employed and paid by a Chinese research university — a fact that he hid from his university and federal agencies," said Assistant Attorney General Demers for National Security. "Any potential conflicts of commitment by a researcher must be disclosed as required by law and university policies. The Department will continue to pursue any unlawful failure to do so."

The indictment alleges that in May 2018 Tao signed a five-year contract with Fuzhou University in China that designated him as a Changjiang Scholar Distinguished Professor. The contract required him to be a full time employee of the Chinese university. While Tao was under contract with Fuzhou University, he was conducting research at KU that was funded through two U.S. Department of Energy contracts and four National Science Foundation contracts.

Kansas Board of Regents' policy requires staff to file an annual conflict of interest report. In Tao's reports to KU, he falsely claimed to have no conflicts of interest. The indictment alleges that he fraudulently received more than $37,000 in salary paid for by the Department of Energy and the National Science Foundation.

If convicted, he faces up to 20 years in federal prison and a fine up to $250,000 on the wire fraud count, and up to 10 years and a fine up to $250,000 on each of the program fraud counts.

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 University of Kansas cooperated and assisted in the FBI's investigation. Assistant U.S. Attorney Tony Mattivi is prosecuting.

In all cases, defendants are presumed innocent until and unless proven guilty. The

indictments merely contain allegations of criminal conduct.

# # #

NSD

19-888

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: Raimondi, Marc (OPA)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi
To: Levi, William (OAG)
Sent: July 22, 2019 11:37 AM (UTC-04:00)

Will, can you please give me a call on this.

Thanks

From: Levi, William (OAG) <(b) (6)
Sent: Monday, July 22, 2019 10:43 AM
To: Gauhar, Tashina (ODAG) <(b) (6) Raimondi, Marc (OPA) <(b) (6)
DuCharme, Seth (OAG) <(b) (6) O'Callaghan, Edward C. (ODAG)
<(b) (6) Hovakimian, Patrick (ODAG) <(b) (6)
Cc: Hornbuckle, Wyn (OPA) <(b) (6) Kupec, Kerri (OPA) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Can CRM also look at (b) (5)

From: Gauhar, Tashina (ODAG) <(b) (6)
Sent: Monday, July 22, 2019 10:41 AM
To: Raimondi, Marc (OPA) <(b) (6) DuCharme, Seth (OAG) <(b) (6)
O'Callaghan, Edward C. (ODAG) <(b) (6) Hovakimian, Patrick (ODAG)
<(b) (6) Levi, William (OAG) <(b) (6)
Cc: Hornbuckle, Wyn (OPA) <(b) (6) Kupec, Kerri (OPA) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Adding Will and Pat to the chain. (I forwarded the documents separately). Thanks.

From: Raimondi, Marc (OPA) <(b) (6)
Sent: Monday, July 22, 2019 10:04 AM
To: DuCharme, Seth (OAG) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6)
O'Callaghan, Edward C. (ODAG) <(b) (6)
Cc: Hornbuckle, Wyn (OPA) <(b) (6) Kupec, Kerri (OPA) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Team, please see attached NSD cleared responses to questions and guidance request from the Washington Post. Our goal is (b) (5)
. I believe (b) (5)
.

I would like to get these remarks back to the Washington Post by noonish so we can make it in the online article that is going up today.

Respectfully,
Marc

From: Hsu, Spencer <(b) (6)
Sent: Friday, July 19, 2019 12:08 PM
To: Raimondi, Marc (OPA) <(b) (6)
Cc: Mangum, Anela (OPA) <(b) (6) Kjergaard, Alison (OPA) <(b) (6)
Koroma, Kadia (USADC) <(b) (6)
Subject: Re: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Thanks Marc, and everyone.

Here's the thrust.

The article describes Shi's case as the latest in a growing list of Justice Department prosecutions of trade secret theft and commercial spying that are part of the Trump administration's effort to stanch what officials say is a systematic campaign by China to steal its way to economic dominance.

Shi's defense says that prosecutors targeted an innocent man, complaining of an overzealous focus on Chinese-Americans whose work or scientific research exposes them to suspicions that they are spying on behalf of Beijing, regardless of whether their efforts are government-directed or involve secret or sensitive technology.

Story notes that countering Chinese trade policies and security threats has been a top priority for both the Trump and Obama administrations, with the current White House decrying Beijing's "economic aggression" in acquiring intellectual property and targeting emerging high-technology industries, among other policies.

1) is this accurate, any concerns:

More than 90 percent of U.S. indictments since 2011 alleging economic espionage to benefit a state involve China, as well as more than two-thirds of trade secret theft cases, although not all included proof that Beijing directed the theft, Justice Department officials said. Prosecutions under the Economic Espionage Act have doubled since 2013 compared with the previous seven years, 22 versus 10.

2) Is this accurate, any concerns.

The crackdown has led to some high-profile failures. Between late 2014 and 2017, prosecutors dropped charges against two former Eli Lilly & Co. scientists, Guoqing Cao and Shuyu Li, accused of passing stolen drug trade secrets to a Chinese company; and against National Weather Service hydrologist Sherry Chen, accused in Ohio of downloading sensitive data on dams. They also asked to dismiss a case against Temple University physicist Xiaoxing Xi who was accused of wire fraud involving the exploitation of technology to help China; and against dual Chinese-Canadian citizen Dong Liu, who had been accused of trying to steel secrets from a Boston medical robotics company.

Since 2009, Asian Americans have been twice as likely as other Americans to be the subject of failed prosecutions for economic spying, a 2017 study by Committee of 100 found.

3) Same

Meanwhile, the Justice Department has given prosecutors in Washington greater oversight and control over national security cases to quell allegations that Chinese-Americans were being wrongly singled out.

Below is argument of critics.

Some defense attorneys and activists say a pattern has continued with U.S. prosecutors bringing cases in which they fail to fully understand the science or overstate the trade secrets in dispute. Without minimizing what the administration calls the unmatched threat of China's "malign behaviors" to American innovation and security, they say that the department's appetite for prosecutions is fueling a new economic cold war, casting suspicion over Americans of Chinese descent trying legitimately to conduct research and do business in China, without drawing bright lines about what information is sensitive and what links to government entities are red flags.

Frank Wu, former dean of the University of California Hastings College of Law and president of the Committee of 100, a nonprofit organization of Chinese American leaders, said the challenge is not new, reviving a debate raised 20 years ago when a federal grand jury indicted Wen Ho Lee, a Taiwanese-American scientist at the Los Alamos National Laboratory on charges of stealing nuclear secrets for China.

Lee was ultimately convicted of one count of mishandling sensitive documents while 58 other counts were dropped. A federal judge apologized in releasing him after 278 days in solitary confinement.

"There are people of Chinese descent who have broken the law who should be prosecuted and punished," Wu said. But, said Wu, whose group conducted the 2017 study, added, "There are also people of Chinese descent who appear to have been targeted because of their national origin or ethnicity and have the book thrown at them... They are cases of disproportionate punishment."

Welcome any thoughts, concerns, suggestions.

Spencer

Spencer Hsu
The Washington Post
M: (b) (6)
O: (b) (6)

From: Raimondi, Marc (OPA) <(b) (6)
Sent: Friday, July 19, 2019 10:40 AM
To: Hsu, Spencer <(b) (6)
Cc: Mangum, Anela (OPA) <(b) (6) Kjergaard, Alison (OPA) <(b) (6) Koroma, Kadia (USADC) <(b) (6)
Subject: Re: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Sure. Be helpful if you could send some questions so I can start answering them. I have very limited availability today to deal with this last minute deadline request.
On Jul 19, 2019, at 10:35 AM, Hsu, Spencer <(b) (6) wrote:

Thanks. I'm heading into a greg craig status hearing, can we talk at noon or 1?

From: Raimondi, Marc (OPA) <(b) (6)
Sent: Friday, July 19, 2019 10:28:25 AM
To: Hsu, Spencer <(b) (6) Mangum, Anela (OPA) <(b) (6) Kjergaard, Alison (OPA) <(b) (6)
Cc: Koroma, Kadia (USADC) <(b) (6)
Subject: Re: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

CAUTION: EXTERNAL SENDER

Yes. What can I help you with?

Marc Raimondi
U.S. Department of Justice
(b) (6)
Mobile (b) (6)
Sent from an iPhone, pls excuse typos and errant autocorrects.

On Jul 19, 2019, at 10:15 AM, Hsu, Spencer <(b) (6) wrote:

Hi Marc, hi Kadia,

So I've been in touch with Kadia to run our trial story by USAO DC today for US v Shan Shi 17cr110, which looks like it will reach a jury next week. Marc, because much/most of the story talks about the wider China initiative, and pushback from some defense attorneys and Chinese American advocates, can/should I run those by you this afternoon?

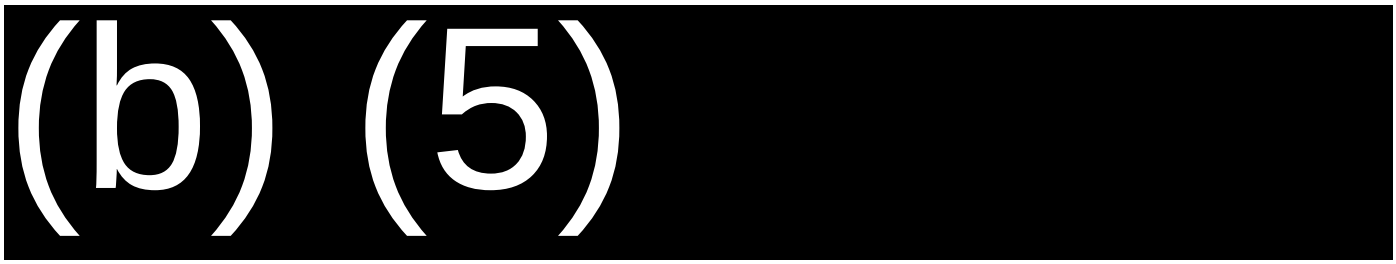
Ellen Nakashima and I are working on the story, she spoke with Anela at the top of the month and we have the "Attorney General China Initiative Fact Sheet" listing info, AAG Demers bio and China related criminal cases since Jan. 2018.

Thank you!

best, Spencer

Spencer Hsu
The Washington Post
M: (b) (6)
O: (b) (6)

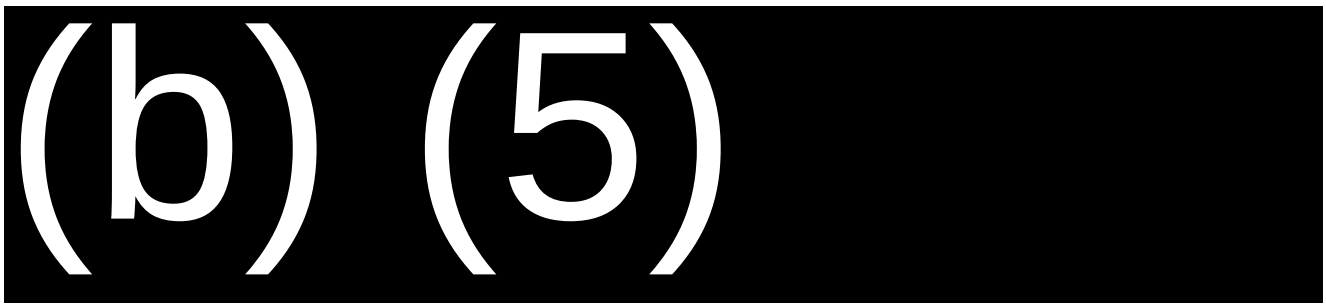
The article describes Shi's case as the latest in a growing list of Justice Department prosecutions of trade secret theft and commercial spying that are part of the Trump administration's effort to stanch what officials say is a systematic campaign by China to steal its way to economic dominance.



Shi's defense says that prosecutors targeted an innocent man, complaining of an overzealous focus on Chinese-Americans whose work or scientific research exposes them to suspicions that they are spying on behalf of Beijing, regardless of whether their efforts are government-directed or involve secret or sensitive technology.

We'll let the evidence speak for itself in this pending prosecution and await the jury's verdict.

Story notes that countering Chinese trade policies and security threats has been a top priority for both the Trump and Obama administrations, with the current White House decrying Beijing's "economic aggression" in acquiring intellectual property and targeting emerging high-technology industries, among other policies.



1) is this accurate, any concerns:

More than 90-percent of U.S. indictments since 2011 alleging economic espionage to benefit a state involve China, as well as more than two-thirds of trade secret theft cases, although not all included proof that Beijing directed the theft, Justice Department officials said. Prosecutions under the Economic Espionage Act have doubled since 2013 compared with the previous seven years, 22 versus 10.

(b) (5)

2) Is this accurate, any concerns.

The crackdown has led to some high-profile failures. Between late 2014 and 2017, prosecutors dropped charges against two former Eli Lilly & Co. scientists, Guoqing Cao and Shuyu Li, accused of passing stolen drug trade secrets to a Chinese company; and against National Weather Service hydrologist Sherry Chen, accused in Ohio of downloading sensitive data on dams. They also asked to dismiss a case against Temple University physicist Xiaoxing Xi who was accused of wire fraud involving the exploitation of technology to help China; and against dual Chinese-Canadian citizen Dong Liu, who had been accused of trying to steel secrets from a Boston medical robotics company.

(b) (5)

Since 2009, Asian Americans have been twice as likely as other Americans to be the subject of failed prosecutions for economic spying, a 2017 study by Committee of 100 found.

(b) (5)

3) Same

Meanwhile, the Justice Department has given prosecutors in Washington greater oversight and control over national security cases to quell allegations that Chinese-Americans were being wrongly singled out.

(b) (5)

Below is argument of critics.

Some defense attorneys and activists say a pattern has continued with U.S. prosecutors bringing cases in which they fail to fully understand the science or overstate the trade secrets in dispute.

(b) (5) **We make prosecutorial decisions based on facts, evidence, and the even-handed application of the law.**

Without minimizing what the administration calls the unmatched threat of China's "malign behaviors" to American innovation and security, they say that the department's appetite for prosecutions is fueling a new economic cold war, casting suspicion over Americans of Chinese descent trying legitimately to conduct research and do business in China, without drawing bright lines about what information is sensitive and what links to government entities are red flags.

The Department of Justice conducts its investigations and prosecutions impartially, without regard to ethnicity of subjects. (b) (5) **.**

Frank Wu, former dean of the University of California Hastings College of Law and president of the Committee of 100, a nonprofit organization of Chinese American leaders, said the challenge is not new, reviving a debate raised 20 years ago when a federal grand jury indicted Wen Ho Lee, a Taiwanese-American scientist at the Los Alamos National Laboratory on charges of stealing nuclear secrets for China.

Lee was ultimately convicted of one count of mishandling sensitive documents while 58 other counts were dropped. A federal judge apologized in releasing him after 278 days in solitary confinement.

"There are people of Chinese descent who have broken the law who should be prosecuted and punished," Wu said. But, said Wu, whose group conducted the 2017 study, added, "There are also people of Chinese descent who appear to have been targeted because of their national origin or ethnicity and have the book thrown at them... They are cases of disproportionate punishment."

We agree with Mr. Wu that people who break the law should be held accountable for their actions and remain committed to vigorously, and impartially, investigating and prosecuting the multi-billion dollar economic thefts targeting American corporations from China.

From: Levi, William (OAG)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi
To: Gauhar, Tashina (ODAG)
Sent: July 22, 2019 10:44 AM (UTC-04:00)

Great thanks. I just copied and pasted to whole group, too.

From: Gauhar, Tashina (ODAG) <(b) (6)
Sent: Monday, July 22, 2019 10:43 AM
To: Levi, William (OAG) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Not sure if you are also sending to the group, so passed the below to Marc.

From: Levi, William (OAG) <(b) (6)
Sent: Monday, July 22, 2019 10:39 AM
To: Gauhar, Tashina (ODAG) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Looks fine. But CRM should look at (b) (5) .

From: Gauhar, Tashina (ODAG) <(b) (6)
Sent: Monday, July 22, 2019 10:37 AM
To: Levi, William (OAG) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Will do. Thanks.

From: Levi, William (OAG) <(b) (6)
Sent: Monday, July 22, 2019 10:36 AM
To: Gauhar, Tashina (ODAG) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

I can review. I'd keep him on the chain too. Thanks!

From: Gauhar, Tashina (ODAG) <(b) (6)
Sent: Monday, July 22, 2019 10:22 AM
To: Levi, William (OAG) <(b) (6)
Subject: FW: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

I know Seth is out this week. Would you like me to add you or someone else from OAG in your absence? I checked in Demers has reviewed and cleared. Thanks.

From: Raimondi, Marc (OPA) <(b) (6)
Sent: Monday, July 22, 2019 10:04 AM
To: DuCharme, Seth (OAG) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6)

O'Callaghan, Edward C. (ODAG) <(b) (6)
Cc: Hornbuckle, Wyn (OPA) <(b) (6) Kupec, Kerri (OPA) <(b) (6)
Subject: RE: Wash Post deadline query today for story online Monday/print Tuesday on China Initiative/trade secrets case v Shan SHi

Duplicative Material, Document ID: 0.7.1536.8211, Bates Number 22cv02001_22-00878_000105

From: Barnett, Gary E. (OAG)
Subject: Speech for press conference on Monday
To: Ankeny, Grant (OAG)
Sent: January 27, 2019 8:53 PM (UTC-05:00)
Attached: 190128 China Press Conference v3 +ash.docx, ATT00001.htm

Most current draft attached. Will have a somewhat updated draft at the 8:45 am prep tomorrow.

From: Stafford, Steven (OPA)
Subject: RE: A/AG remarks
To: Barnett, Gary E. (OAG)
Sent: January 27, 2019 5:22 PM (UTC-05:00)
Attached: 190128 China Press Conference v3.docx
Didn't know that we have 2 indictments. Updated

_____
Steven J. Stafford
U.S. Department of Justice

-----Original Message-----
From: Stafford, Steven (OPA)
Sent: Sunday, January 27, 2019 4:19 PM
To: Barnett, Gary E. (OAG) <(b) (6)
Subject: RE: A/AG remarks

Just circulated to Hickey, CRM, Kerri

_____
Steven J. Stafford
U.S. Department of Justice

-----Original Message-----
From: Barnett, Gary E. (OAG) <(b) (6)
Sent: Sunday, January 27, 2019 2:04 PM
To: Stafford, Steven (OPA) <(b) (6)
Subject: Re: A/AG remarks

Great. Thanks.

> On Jan 27, 2019, at 2:03 PM, Stafford, Steven (OPA) <(b) (6) wrote:
>
> Almost done. Will circulate shortly
>
> _____
> Steven J. Stafford
> U.S. Department of Justice
>
>
> -----Original Message-----
> From: Barnett, Gary E. (OAG) <(b) (6)
> Sent: Sunday, January 27, 2019 2:00 PM
> To: Stafford, Steven (OPA) <(b) (6)
> Subject: A/AG remarks
>
> Hey Stafford, welcome back. Hope the shutdown wasn't too boring.
>
> Is there a draft of the A/AG'a remarks for tomorrow's press conference?
>
> Thanks,
> Gary

From: Hickey, Adam (NSD)
Subject: China Initiative and Case
To: Levi, William (OAG)
Sent: December 17, 2018 10:09 AM (UTC-05:00)
Attached: NSD Demers Testimony for SJC China Non-Trad Espionage_12.12.18.pdf, Subcasino Indictment v.18 (myc).docx, APT10 Indictment PR v.5 (clean).docx

Will,

Here's a link to the Fact Sheet on the China Initiative:

https://www.justice.gov/opa/speech/file/1107256/download

John's testimony is attached.

The draft press release and indictment are attached (b)(5) per NSD I will call you with the password.

Adam

Department of Justice

STATEMENT OF

JOHN C. DEMERS
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

FOR A HEARING ON

CHINA'S NON-TRADITIONAL ESPIONAGE AGAINST THE UNITED STATES: THE THREAT AND POTENTIAL POLICY RESPONSES

PRESENTED ON

DECEMBER 12, 2018

Statement of John C. Demers
Assistant Attorney General, National Security Division
U.S. Department of Justice
Before the Committee on the Judiciary
United States Senate
December 12, 2018

Good morning Chairman Grassley, Ranking Member Feinstein, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice (Department) concerning China's economic aggression, its efforts to threaten our national security on several, non-traditional fronts, and our efforts to combat them. The Department views this threat as a priority, and last month the former Attorney General announced an initiative to marshal our resources to better address it. This initiative continues, and I am privileged to lead this effort on behalf of the Department. I especially appreciate the Committee's interest in this area of growing concern.

I will begin by framing China's strategic goals, including its stated goal of achieving superiority in certain industries, which, not coincidentally, corresponds to thefts of technology from U.S. companies in those industries. I will then describe some of the unacceptable methods by which China is pursuing (or could pursue) those goals at our expense. Finally, I will explain what the Department is doing about it, including through our China Initiative.

I. China's Strategic Goals

Official publications of the Chinese government and the Chinese Communist Party set out China's ambitious technology-related industrial policies. These policies are driven in large part by China's goals of dominating its domestic market and becoming a global leader in a wide range of technologies, especially advanced technologies. The industrial policies reflect a top-down, state-directed approach to technology development and are founded on concepts such as "indigenous innovation" and "re-innovation" of foreign technologies, among others. The Chinese government regards technology development as integral to its economic development and seeks to attain domestic dominance and global leadership in a wide range of technologies for economic and national security reasons. In pursuit of this overarching objective, China has issued a large number of industrial policies, including more than 100 five-year plans, science and technology development plans, and sectoral plans over the last decade.[1]

In 2015, China's State Council released the "Made in China 2025 Notice," a ten-year plan for targeting ten strategic advanced technology 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

[1] Office of the U.S. Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 14-17 (Mar. 22, 2018), *available at* https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

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 so, China has committed to pursuing an "innovation-driven" development strategy and prioritizing breakthroughs in higher-end innovation. But that is only part of the story: "Made in China 2025" is as much roadmap to theft as it is guidance to innovate.

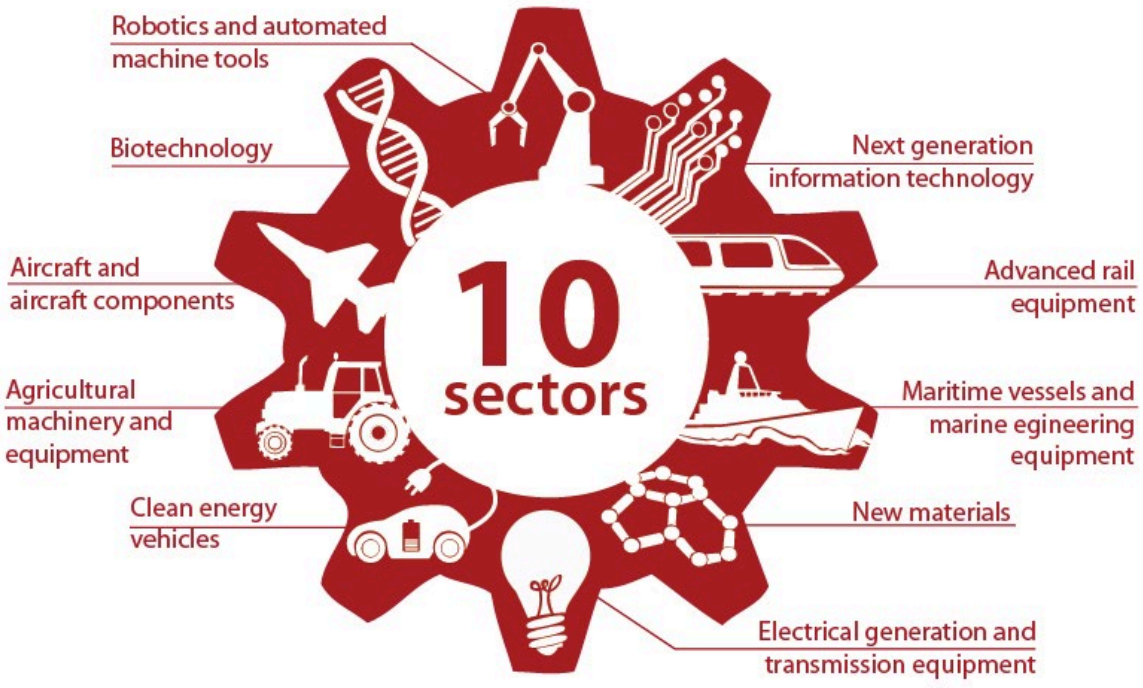


FIGURE 1: "MADE IN CHINA 2025" TARGETS 10 STRATEGIC INDUSTRIES FOR DEVELOPMENT (NSD).

No one begrudges a nation that generates the most innovative ideas and from them develops the best technology. But we cannot tolerate a nation that steals our firepower and the fruits of our brainpower. And this is just what China is doing to achieve its development goals. While China aspires to be a leading nation, it does not act like one. China is instead pursuing its goals through malign behaviors that exploit features of a free-market economy and an open society like ours. As depicted in Figure 2 (and described in more detail below), China is using a variety of means, ranging from the facially legal to the illicit, including various forms of economic espionage, forced technology transfer, strategic acquisitions, and other, less obvious tactics to advance its economic development at our expense.

Non-Traditional Collectors	China uses individuals for whom science or business is their primary profession to target and acquire US technology.
Joint Ventures (JV)	China uses JVs to acquire technology and technical know-how.
Research partnerships	China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities.
Academic Collaborations	China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps.
S&T Investments	China has sustained, long-term state investments in its S&T infrastructure.
M&A	China seeks to buy companies that have technology, facilities and people. These sometimes end up as Committee on Foreign Investment in the United States (CFIUS) cases.
Front Companies	China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology.
Talent Recruitment Programs	China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs.
Intelligence Services	The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts.
Legal and Regulatory Environment	China uses its laws and regulations to disadvantage foreign companies and advantage its own companies.

FIGURE 2: CHINA'S STRATEGIC GOALS (COURTESY OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE).

This multifaceted approach by China requires a whole-of-government response by the United States. While some of China's tactics violate criminal laws, not all of them do, and even the violations may be difficult to detect and the offenders even more difficult to apprehend. For this reason, the Department must follow the same approach here that we follow with terrorism or classic espionage: we must cultivate traditional law enforcement responses (like investigations and prosecutions or civil suits) to disrupt specific actors while at the same time supporting other

departments and their authorities in a long-term, whole-of-government effort to raise the costs of bad behavior and advance the Administration's national security strategy.

II. Economic Espionage and Trade Secret Theft

Espionage, as that term is traditionally used, involves trained intelligence professionals seeking out national defense information, typically contained in classified files. State-on-state spycraft conducted by intelligence services has existed for millennia, and we will continue to do our best to fight it. In fact, the Department now has three pending cases against former U.S. intelligence officers who are alleged to have spied for China—which is an unprecedented number.

But China now uses the same intelligence services and the same tradecraft—from co-opting insiders, to sending non-traditional collectors, to effectuating computer intrusions—against American companies and American workers to steal American technology and American know-how. Our private sector is at grave risk from the concerted efforts and resources of a determined nation-state.

Our recent cases bear this out. Over the course of just a few months, the Department's National Security Division (NSD) and U.S. Attorney's Offices across the country announced three cases alleging crimes committed 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, Yanjun Xu, who allegedly sought technical information about jet aircraft engines from leading aviation companies in the United States and elsewhere. To get this information, he is accused of concealing the true nature of his employment and recruiting 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. Fortunately, thanks to swift action by one of the companies he targeted, we were able to identify Xu and build a criminal case while helping the company protect its intellectual property. And thanks to close cooperation from our foreign law enforcement partners in Belgium, where Xu traveled for business, we secured his arrest and extradition to the United States.

- That same month, the Department unsealed charges in another case targeting commercial aviation technology. According to that indictment, JSSD officers managed 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. Meanwhile, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere, and the stolen data could save the Chinese company substantial research and development expenses. And to accomplish their objectives, the conspirators successfully co-opted at least two Chinese nationals employed by one of the companies, 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.

Our private sector finds itself the target of one of the most well-resourced nation-states in history and tactics that go far beyond the normal rough and tumble of capitalism. American businesses need the backing of the U.S. government to survive this threat.

As these cases also illustrate, to find what the Chinese are after one need look no further than the "Made in China 2025" initiative: from underwater drones and autonomous vehicles to global navigation satellite systems used in agriculture, from the steel industry to nuclear power plants and solar technology, from critical chemical compounds to inbred corn seeds. Chinese thefts target all kinds of commercial information, including trade secrets, as well as goods and services whose exports are restricted because of their military use.

From 2011-2018, more than 90 percent of the Department's cases alleging economic espionage by or to benefit a state involve China, and more than two-thirds of the Department's theft of trade secrets cases have had a nexus to China. To be sure, in this second category, there have been cases in which we did not have admissible proof that the Chinese government 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, over half its global workforce. Another recent example 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. And while we could not prove in court that these thefts were directed by the Chinese government, there is no question that they are in perfect consonance with Chinese government economic policy. 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 amply justify the conclusion that the Chinese government is ultimately responsible for those thefts, too.

In all of these cases, China's strategy is the same: rob, replicate, and replace. Rob the American company of its intellectual property, replicate the technology, and replace the American company in the Chinese market and, one day, the global market. One of the best illustrations of this is the recent Micron case.

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. 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, *which were based on the very technology it is accused of stealing.*

For now, we may have mitigated the damage to Micron. 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. And, in addition to the criminal indictment, we sued both the Chinese and Taiwan competitors, seeking an injunction that would bar them from exporting any products based on the stolen technology to the United States.

But the case has revealed gaps in the statutes we use to protect companies like Micron. For one thing, our ability to prosecute trade secret theft depends on having either a U.S. defendant or proof that an act in furtherance of the offense took place within the United States. 18 U.S.C. § 1837. Here, the defendants are accused of accessing trade secrets stored on Micron's systems within the United States, but I can easily imagine circumstances where a U.S. company is robbed abroad, and criminal charges are unavailable here. And although one ex-Micron employee is accused of removing hundreds of the company's files from its servers in the United States, without authorization and to benefit its competitor, and of running software to mask his activities, we could not charge him with a computer crime under Ninth Circuit precedent. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

III. Foreign Direct Investment and Supply Chain Threats

While theft is a major concern, it is not the only vector China can use to achieve its goals at the expense of our national security. Through its direct investment in U.S. companies and its sales of goods and services to our telecommunications sector, among others, China has sought to exploit our open markets for its national security gain. Both of these predatory Chinese tactics present a corresponding national security risk for the United States.

First, although we welcome foreign investment, we must be wary that what can be stolen can also, often, be bought. NSD's Foreign Investment Review Staff represents the Department on the Committee on Foreign Investment in the United States (CFIUS), and the Committee's work addresses the threat posed to our country through certain foreign investment from China where other U.S. Government authorities are not sufficient. China has been a rapidly expanding investor in the United States, becoming the largest single source of CFIUS filings in the last few years. While foreign direct investment helps our economy, some investments do pose an unacceptable national security risk.

Last year, for example, an investor owned and controlled by the Chinese government sought a $1.3 billion acquisition of Lattice Semiconductor Corporation, a chipmaker whose products are used by the U.S. government. The President prohibited the transaction, citing the national security risk posed by the deal. Earlier this year, the President blocked the attempted hostile takeover of the semiconductor and telecommunications equipment company Qualcomm by Broadcom. His action was based on the national security risks presented by such an acquisition, as detailed by the Department and others before CFIUS.

Technology transfer, particularly that which could violate export controls, can be a national security concern, but so can access to personal information, even that which initially appears to have no connection to national security. Increasingly, the Department has reviewed foreign investments with an eye towards protecting personal identifying information, health information, and other sensitive electronic information, which can be used to target individuals for espionage, especially if large datasets can be cross-referenced. As more devices are connected to the Internet, and more data is collected, it becomes possible to use that information for purposes never foreseen or intended. As one story from the last year illustrates, what looks like a map of fitness trackers might be a key to identifying national security installations; and the street you grew up on and the name of your first pet could be the clues to access your e-mail account (or more). Accordingly, as the Department has served as a co-lead agency in CFIUS in an increasing number of cases during this Administration, we bring to bear the Department's understanding of how privacy, data security and integrity, and the rule of law can implicate national security in evaluating transactions for national security risk.

Second, we are increasingly concerned with supply chain threats, especially to our telecommunications sector. In July, the Administration recommended that the Federal Communications Commission (FCC) 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 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."

IV. The Department's China Initiative

As these prosecutions and other actions show, the Department has long taken the threat from China seriously and worked to confront it. But they also show the diversity and magnitude of the challenges we face and the need to prioritize our response. I will close by describing the purpose of the Department's China Initiative and some of its principal goals.

Broadly speaking, the China Initiative aims to raise awareness of the threats we face, to focus the Department's resources in confronting them, and to improve the Department's response, particularly to newer challenges. I will chair a Steering Group, composed of my

counterpart in the Criminal Division, Assistant Attorney General Brian Benczkowski, the Federal Bureau of Investigation's (FBI) Executive Assistant Director for National Security Jay Tabb, and five U.S. Attorneys, from Alabama, California, Massachusetts, New York, and Texas, to direct its efforts. We convened for the first time recently, and we have begun our work.

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. We will share enforcement approaches and best practices across the country. But as important as it is to investigate and prosecute trade secret theft like the kind I have described here, we must broaden our approach.

- First, we need to adapt our enforcement strategy to reach 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;

- Second, we will work with U.S. Attorneys and their Assistants across the country to develop a broad outreach campaign to engage with companies, universities, and others in their Districts, both to raise awareness of the kinds of the threats I have described and to reinforce the trust that leads to cooperation with law enforcement and the enforcement actions I have described. (Congress, too, can help raise whole-of-society awareness through outreach to constituents, businesses, and universities.);

- Third, we will identify violations of the Foreign Corrupt Practices Act by Chinese companies, to the disadvantage of American firms they compete with;

- Fourth, we will continue to work to improve Chinese responses to our requests for assistance in criminal investigations and prosecutions under the Mutual Legal Assistance Agreement we have with China; and

- Finally, as the Micron case shows, among others, in addition to making good cases, we must look for ways our investigations can be properly leveraged to support our federal partners' tools, 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.

The second prong of our China Initiative is focused on preventing threats from without, through foreign investments and supply chain compromises. The Administration was pleased to support recent legislation, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which adapts CFIUS to address current threats. We look forward to working with the Department of the Treasury to implement the newly launched pilot program under the statute, and to developing regulations to implement appropriately CFIUS's expanded authority, and processes for the long-term success of the Committee in light of increased workflows. 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 should continue to explore ways to make this process more efficient and expedient. Team Telecom reform is clearly needed. And we will work with our interagency and foreign partners on a strategy to ensure the security of our telecommunications networks as we transition to 5G.

Finally, we are cognizant that China's game is a long one, and that it is working to covertly influence American public opinion in its favor. As the Vice President recently said, quoting the Intelligence Community, "China is targeting U.S. state and local governments and officials to exploit any divisions between federal and local levels on policy. It's using wedge issues, like trade tariffs, to advance Beijing's political influence." At the Department, we are concerned that Beijing may use its economic leverage over businesses to covertly influence American policy, may covertly influence student groups on campus to monitor or retaliate against fellow students, or may exercise undisclosed control over media organizations in the United States, all without proper registration under the Foreign Agents Registration Act (FARA) and the accountability it brings. Under the Initiative, we will work to educate colleges and universities about potential threats to academic freedom and open discourse from covert Chinese influence efforts, raise awareness among the business community that acting as the covert agent of the Chinese government could trigger obligations to register under FARA, and continue to evaluate foreign media organizations for compliance with FARA.

In all of these efforts, we will be alert to ways that legislative reform may be helpful, and my staff and I would welcome the opportunity to work with the Congress on these issues.

Done well, our China Initiative will not only improve the way law enforcement responds to China's economic aggression, but also will raise our country's awareness of the threats and how we as a people can work to protect ourselves and our assets from them.

***

Even a whole-of-Executive-Branch effort will not succeed alone, however. We must work together with you in the Congress, as well as with the private sector, academic institutions, and foreign partners. For this reason, I am grateful to the Committee for providing me the opportunity to discuss these important issues on behalf of the Department, and for working with us to bring attention to and counter this national security threat. I am happy to answer any questions you may have.

From: Raimondi, Marc (OPA)
Subject: RE: AG's remarks
To: Tucker, Rachael (OAG); Hemann, John (USACAN); Hickey, Adam (NSD); [redacted] (NSD); Stafford, Steven (OPA); Demers, John C. (NSD); Kupec, Kerri (OPA); Flores, Sarah Isgur (OPA); Hornbuckle, Wyn (OPA)
Cc: Mangum, Anela (OPA)
Sent: November 1, 2018 10:39 AM (UTC-04:00)
Attached: 2018 11 01 1034 AG Remarks China Initiative clean.docx, 2018 11 01 1034 AG Remarks China Initiative Show Edits.docx

Team, added an additional NSD edit, it is in show changes and the clean version, please discard previous versions and make any additional edits to this one. The time date stamps in the name of the document have been updated to help with version control.

From: Tucker, Rachael (OAG)
Sent: Thursday, November 01, 2018 10:16 AM
To: Raimondi, Marc (OPA) <[redacted] Hemann, John (USACAN) <[redacted] Hickey, Adam (NSD) [redacted]; Stafford, Steven (OPA) <[redacted] Demers, John C. (NSD) [redacted]; Kupec, Kerri (OPA) <[redacted] Flores, Sarah Isgur (OPA) <[redacted] Hornbuckle, Wyn (OPA) <[redacted]
Cc: Mangum, Anela (OPA) <[redacted]
Subject: RE: AG's remarks

Let me confirm with that he didn't make any additional edits last night. Whatever edits he makes will be added on top of this draft. Will be in touch.

From: Raimondi, Marc (OPA)
Sent: Thursday, November 1, 2018 10:15 AM
To: Hemann, John (USACAN) <[redacted] Hickey, Adam (NSD) [redacted]; [redacted] >; Stafford, Steven (OPA) <[redacted] Demers, John C. (NSD) [redacted]; Tucker, Rachael (OAG) <[redacted] Kupec, Kerri (OPA) <[redacted] Flores, Sarah Isgur (OPA) <[redacted] Hornbuckle, Wyn (OPA) <[redacted]
Cc: Mangum, Anela (OPA) <[redacted]
Subject: RE: AG's remarks
Importance: High

Team, this is what I believe and much hope to be the final AG remarks. This is the version that Adam Hickey edited, Steve Stafford accepted the edits and John Hemann made a couple additional factual edits which I incorporated. All the edits from Adam and me are in the show change copy.

Steve or Rachel, please confirm that this is the final so we can start printing for press kits.

Best,
Marc

From: Hemann, John (USACAN) <[redacted]
Sent: Thursday, November 01, 2018 10:11 AM
To: Raimondi, Marc (OPA) <[redacted]
Cc: Hickey, Adam (NSD) [redacted]; Stafford, Steven (OPA) <[redacted]
Subject: Re: AG's remarks

Perfect.

Sent from my iPhone

On Nov 1, 2018, at 10:10 AM, Raimondi, Marc (OPA) <(b) (6) wrote:

> John, I am not sure you were working off of the latest set of remarks from the AG. Regardless, I will make the edit to the sentence you reference so it reads that (b) (5) .
>
> Does this work for the first nit?
>
> Revised: (b) (5)
>
> Original
> (b) (5)
>
> -----Original Message-----
> From: Hemann, John (USACAN) <(b) (6)
> Sent: Thursday, November 01, 2018 9:37 AM
> To: Raimondi, Marc (OPA) <(b) (6)
> Cc: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD >; (b)(6), (b)(7)(C) per NSD >
> Subject: AG's remarks
>
> Two nits in AG's remarks:
>
> (b) (5)
> .
>
> Also, (b) (5)
>
> Sent from my iPhone

From: (b)(6) Rachael Tucker (OAG)
Subject: Fwd: Updated AG remarks
To: Allen, Alexis (OAG)
Sent: November 1, 2018 8:32 AM (UTC-04:00)
Attached: 181031 1830 China v4 + JAE.docx, ATT00001.htm

Begin forwarded message:

From: "Hickey, Adam (NSD)" (b)(6), (b)(7)(C) per NSD
Date: October 31, 2018 at 9:09:24 PM EDT
To: "Stafford, Steven (OPA)" <(b) (6)
Cc: "Tucker, Rachael (OAG)" <(b) (6) (b)(6), (b)(7)(C) per NSD "Raimondi, Marc (OPA)" <(b) (6) "Flores, Sarah Isgur (OPA)" <(b) (6) "Gauhar, Tashina (ODAG)" <(b) (6) "Groves, Brendan M. (ODAG)" <(b) (6) "Demers, John C. (NSD)" (b)(6), (b)(7)(C) per NSD
Subject: RE: Updated AG remarks

Sorry – please use this one (three additional changes total).

From: Hickey, Adam (NSD)
Sent: Wednesday, October 31, 2018 9:06 PM
To: Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD
Cc: Stafford, Steven (OPA) <(b) (6) Tucker, Rachael (OAG) <(b) (6) (b)(6), (b)(7)(C) per NSD Raimondi, Marc (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) Groves, Brendan M. (ODAG) <(b) (6)
Subject: RE: Updated AG remarks

Steve, two other small changes following review by CES. Thanks much.

From: Demers, John C. (NSD)
Sent: Wednesday, October 31, 2018 8:42 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Cc: Stafford, Steven (OPA) <(b) (6) Tucker, Rachael (OAG) <(b) (6) (b)(6), (b)(7)(C) per NSD Raimondi, Marc (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) Groves, Brendan M. (ODAG) <(b) (6)
Subject: Re: Updated AG remarks

That works. Thanks.

On Oct 31, 2018, at 8:41 PM, Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD wrote:

How about this:

(b) (5)

(b) (5)

From: Demers, John C. (NSD)
Sent: Wednesday, October 31, 2018 8:34 PM
To: Stafford, Steven (OPA) <(b) (6)
Cc: Tucker, Rachael (OAG) <(b) (6) Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD Raimondi, Marc (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) Groves, Brendan M. (ODAG) <(b) (6)
Subject: Re: Updated AG remarks

The only comment I have is that (b) (5)

John

On Oct 31, 2018, at 6:47 PM, Stafford, Steven (OPA) <(b) (6) wrote:

> Raimondi—I took all of these edits
>
> Steven J. Stafford
> U.S. Department of Justice

From: Tucker, Rachael (OAG)
Sent: Wednesday, October 31, 2018 6:46 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD Raimondi, Marc (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Stafford, Steven (OPA) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) Groves, Brendan M. (ODAG) <(b) (6)
Subject: RE: Updated AG remarks

Looks good to me.

From: Hickey, Adam (NSD)
Sent: Wednesday, October 31, 2018 6:37 PM
To: Tucker, Rachael (OAG) <(b) (6) Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD Raimondi, Marc (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Stafford, Steven (OPA) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) Groves, Brendan M.

(ODAG) <(b) (6)
Subject: RE: Updated AG remarks

In the interest of time, here are some (small) suggestions. If I have any others (after consulting with CES), I'll pass them on to this group. I think Steve did a nice job with these.

From: Tucker, Rachael (OAG)
Sent: Wednesday, October 31, 2018 6:13 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; (b)(6), (b)(7)(C) per NSD
Raimondi, Marc (OPA) <(b) (6)
Flores, Sarah Isgur (OPA) <(b) (6)
Stafford, Steven (OPA) <(b) (6)
Gauhar, Tashina (ODAG) <(b) (6)
Groves, Brendan M. (ODAG) <(b) (6)
Subject: Updated AG remarks

I haven't reviewed these yet but wanted to circulate what Steve updated after our meeting with the boss today.

<181031 1830 China v4.docx>

From: Hickey, Adam (NSD)
Subject: RE: 2018 10 31 Demers China Initiative
To: Mangum, Anela (OPA); Raimondi, Marc (OPA); Demers, John C. (NSD); Tucker, Rachael (OAG)
Sent: October 31, 2018 6:06 PM (UTC-04:00)
Attached: 2018 10 31 1730 Demers China Initiative +ash.docx

Okay – resending.

From: Mangum, Anela (OPA)
Sent: Wednesday, October 31, 2018 6:06 PM
To: Raimondi, Marc (OPA) <(b) (6) Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; Tucker, Rachael (OAG) <(b) (6)
Subject: RE: 2018 10 31 Demers China Initiative

Of course, I will update the remarks when I get the changes from Adam.

Thank you.

From: Raimondi, Marc (OPA)
Sent: Wednesday, October 31, 2018 5:31 PM
To: Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD; Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; Tucker, Rachael (OAG) <(b) (6)
Cc: Mangum, Anela (OPA) <(b) (6)
Subject: RE: 2018 10 31 Demers China Initiative

No problem Adam, we will make the changes, we didn't print them out yet so we are good.

Anela, can you please accept these edits and update the remarks as released. Can be tomorrow morning.

Thanks much.

From: Hickey, Adam (NSD)
Sent: Wednesday, October 31, 2018 5:29 PM
To: Demers, John C. (NSD) (b)(6), (b)(7)(C) per NSD; Raimondi, Marc (OPA) <(b) (6) Tucker, Rachael (OAG) <(b) (6)
Subject: RE: 2018 10 31 Demers China Initiative

I have a couple critical suggestions to these – sorry.

From: Demers, John C. (NSD)
Sent: Wednesday, October 31, 2018 4:11 PM
To: Raimondi, Marc (OPA) <(b) (6) Tucker, Rachael (OAG) <(b) (6) Hickey, Adam (NSD) (b)(6), (b)(7)(C) per NSD
Subject: 2018 10 31 Demers China Initiative

Marc,

Here is the final. The AG's folks are working his remarks. (b)(5) per NSD

Thanks,
John

From: Gauhar, Tashina (ODAG)
Subject: FW: 2018 10 30 Demers China Initiative.docx
To: Tucker, Rachael (OAG)
Cc: Groves, Brendan M. (ODAG)
Sent: October 31, 2018 1:57 PM (UTC-04:00)
Attached: 2018 10 30 Demers China Initiative.docx, ATT00001.txt

Hi Rachael -- Just checking in on the plans for tomorrow. Let us know if you need anything or we can be of any help.

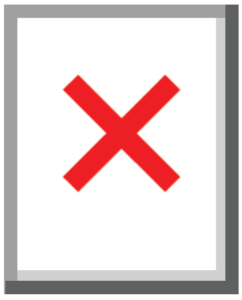
Thanks.

-----Original Message-----
From: Raimondi, Marc (OPA)
Sent: Tuesday, October 30, 2018 10:07 PM
To: Navas, Nicole (OPA) <(b) (6) Flores, Sarah Isgur (OPA) <(b) (6) Hornbuckle, Wyn (OPA) <(b) (6) Kupec, Kerri (OPA) <(b) (6) Mangum, Anela (OPA) <(b) (6) Tucker, Rachael (OAG) <(b) (6) Gauhar, Tashina (ODAG) <(b) (6) (b)(6), (b)(7)(C), (b)(7)(E) per FBI (b)(6), (b)(7)(C), (b)(7)(E) per FBI
Subject: 2018 10 30 Demers China Initiative.docx

Team, here are our final remarks for John Demers for the China announcement.

Marc Raimondi
U.S. Department of Justice
(b) (6)

From: USDOJ-Office of Public Affairs
Subject: THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)
To: Hamilton, Gene (OAG)
Sent: November 16, 2020 11:27 AM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

MONDAY, NOVEMBER 16, 2020

THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)

WASHINGTON --- On the two-year anniversary of the Attorney General's China Initiative, the Department continues its significant focus on the Initiative's goals and announced substantial progress during the past year in disrupting and deterring the wide range of national security threats posed by the policies and practices of the People's Republic of China (PRC) government.

"In the last year, the Department has made incredible strides in countering the systemic efforts by the PRC to enhance its economic and military strength at America's expense," said Attorney General William P. Barr. "While much work remains to be done, the Department is committed to holding to account those who would steal, or otherwise illicitly obtain, the U.S. intellectual capital that will propel the future."

"The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt," said FBI Director Christopher Wray. "The FBI opens a new China-related counterintelligence case nearly every 10 hours and we'll continue our aggressive efforts to counter China's criminal activity."

Established in November 2018, the Initiative identified a number of goals for the Department, ranging from increased focus on the investigation and prosecution of trade secret theft and economic espionage, to better countering threats posed by Chinese foreign investment and supply chain vulnerabilities.

Prioritize investigations of economic espionage and trade secret theft

The Initiative prioritizes use of the Department's core tool, criminal investigation and prosecution, to counter economic espionage and other forms of trade secret theft. In the past year, the Department charged three economic espionage cases (in which the trade secret theft was intended to benefit the Chinese government), bringing the total to five since the China Initiative was first announced. Overall, since the Initiative was announced, we have charged more than 10 cases in which the trade secret theft had some alleged nexus to China, and we obtained guilty pleas of three defendants in those cases over the past year.

To take one example, the Department announced the China Initiative on the same day that it unsealed criminal charges against United Microelectronics (UMC), the Chinese state-owned enterprise Fujian Jinhua, and several individual defendants, for economic espionage that victimized Micron Technology, Inc., a leading U.S. semiconductor company.

"The United Microelectronics case is a glaring example of the PRC's 'rob, replicate, and replace' strategy, in which it robs a U.S. institution of its intellectual capital, replicates the stolen technology, and then endeavors to replace the U.S. institution on the Chinese and then the global market," said John Demers, Assistant Attorney General for National Security. "Thanks to the dedication and diligence of prosecutors and FBI agents, UMC pleaded guilty to criminal trade secret theft and agreed to pay a fine of $60 million, the second largest fine in a trade secret case, and to cooperate in the pending prosecution of its co-defendants."

The National Counterintelligence Task Force, co-led by the FBI, launched its first major campaign in 2020, devoted to protecting U.S. technology and research from the Chinese government and its proxies. This is a further step in the FBI's and Department's efforts to enlist all appropriate partners in ensuring integrity in government-funded programs and defeating economic espionage and theft of trade secrets.

Develop an enforcement strategy for non-traditional collectors

At the outset, the Department identified academia as one of our most vulnerable sectors, because its traditions of openness, and the importance of international exchanges to the free flow of ideas, leave it vulnerable to PRC exploitation. The Department has pursued a two-pronged strategy of raising awareness on campuses of the threats posed by China (and the importance of implementing a security program to detect them) and prosecuting researchers who have deliberately deceived authorities about their ties to China, which deprives institutions of the ability to screen for conflicts of interest and commitment, or otherwise exploited their access.

For example, the PRC has used talent programs to encourage the transfer of technical expertise from the United States, and elsewhere in the world, to benefit the PRC's economic and military development. Talent recruits generally sign contracts with the PRC sponsor-entity that obligate them to produce scientific outputs; to publish the results of their work in the name of the PRC beneficiary; to allow the PRC beneficiary to assert intellectual property rights over their outputs; and to recruit other researchers into the programs, among other obligations.

In exchange, the talent recruits may receive lucrative compensation packages, prestigious titles, and custom-built laboratories.

"While membership in these talent programs is not *per se* illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to

work in the interest of the Chinese Communist Party," said Adam S. Hickey, Deputy Assistant Attorney General, National Security Division.

The Initiative brings together resources from across the Department, including the National Security, Criminal, Tax, and the Civil Divisions to address this unique challenge fairly and effectively. In the past year, Department prosecutors have brought fraud, false statements, tax, smuggling and other charges against ten academics affiliated with research institutions across the country. To date, prosecutors have obtained convictions in three of those cases.

This year, the FBI and Department prosecutors also exposed six individuals, studying in the United States, found to be connected to People's Liberation Army military institutes, who concealed their affiliations from the State Department when applying for research visas to study at U.S. universities. In one of those cases, the Department alleged that a PLA officer was being tasked by superiors in the PRC to obtain information that would benefit PLA operations. In another case, a PLA medical researcher stands accused of following orders to observe lab operations at a U.S. university, which received funding from the U.S. government, in order to replicate those operations in the PRC.

In each of the cases, the defendants are accused of concealing their PLA affiliations in order to obtain visas that allowed them to travel to the United States. After the FBI conducted interviews this summer that led to charges in those cases and the State Department closed the PRC's Houston Consulate, a large number of undeclared, PLA-affiliated Chinese researchers fled the United States.

Those six examples are just part of the interagency effort to protect academia and taxpayer-funded research. The FBI and Department have been collaborating with federal grant-making agencies, the Joint Committee on the Research Environment, the major academic associations, the Academic Security and Counter Exploitation working group, and other appropriate entities, as well as hundreds of individual universities nationwide.

Counter malicious cyber activity

The Department continues to expose and disrupt efforts by the PRC government to steal our intellectual property and our personally identifiable information (PII) through computer intrusions. During the past year, we charged hackers working for the People's Liberation Army with the 2017 Equifax intrusion and others associated with the Ministry of State Security (MSS) in relation to global computer intrusion campaigns targeting biomedical companies conducting COVID-19-related research, engineering firms, and software makers. One such MSS case resulted in the arrest of two conspirators in Malaysia. Two of these cases highlighted China's development into a safe harbor for criminal hackers who also work for the PRC. The Department disrupted these cyber threats in coordination with the private sector, using legal process to seize control of hacking infrastructure while the private sector removed other infrastructure from their platforms.

In May, the FBI, in conjunction with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, also issued a public announcement to raise awareness of the threat to COVID-19 research by PRC-affiliated cyber actors and offer advice on better protecting that research from thefts.

Counter malign foreign influence

The Department has used the Foreign Agents Registration Act ("FARA"), which requires those acting to influence public policy and opinion on behalf of a foreign individual or entity, to improve transparency and expose China's foreign influence efforts. Over the past year, the Department opened a record number of FARA investigations overall and doubled the number of new registrants and new foreign principals registering annually as of 2016. That includes obtaining a record number of registrations from Chinese media companies. The Department also notified a registered Chinese media company that its filings were deficient because they failed to fully disclose its activity in the United States and failed to properly label its informational materials. The media entity remedied those deficiencies shortly thereafter.

Through its outreach efforts to universities, the Department has highlighted the need to protect foreign students studying in the United States from coercive efforts by the Communist Party to censor the freedom of thought and expression that all students here should enjoy.

In late 2019, the FBI's Foreign Influence Task Force formally established a new unit devoted specifically

to understanding and defeating the malign foreign influence threat from the Chinese government and its proxies.

Counter foreign intelligence activities

The Department has achieved a number of successes in the last year in countering China's foreign intelligence activities. China has been targeting former members of the U.S. intelligence community for recruitment, and the Department has been holding accountable individuals who succumb to their efforts. In November 2019, a former CIA case officer was sentenced to 19 years in prison for conspiring to deliver national defense information to the PRC. In August 2020, another former CIA officer who had been tasked by the PRC was arrested on the same charge — the fourth former intelligence officer charged in the last three years for similar conduct.

The Department is particularly focused on disrupting the PRC government from using career networking and social media sites to target Americans, as well as holding those accountable who hide behind fake profiles to co-opt individuals on behalf of the PRC. As one part of this effort, the FBI, in partnership with the National Counterintelligence and Security Center, created an educational film, "The Nevernight Connection," which was released online in September 2020 to educate the public about the Chinese intelligence services' use of social media to spot and recruit persons of interest, especially current or former security clearance holders.

In March 2020, Xuehua (Edward) Peng was sentenced to 48 months in prison, and ordered to pay a $30,000 fine, for acting as an agent of the PRC's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital cards containing classified information from a source in the United States to the MSS operatives in China.

In October 2020, Jun Wei Yeo was sentenced to 14 months in prison for acting within the United States as an agent of the MSS recruiting Americans, including U.S. military and government employees with high-level clearances. Yeo concealed his MSS affiliation from his American targets and used career networking sites and a false consulting firm to lure them to write papers which he ultimately passed to his MSS handlers.

In October 2020, eight defendants were charged with conspiring to act in the United States as illegal agents of the PRC, six of whom also face related charges of conspiring to commit interstate and international stalking. According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate a resident of New Jersey and his family in order to force them to return to the PRC as part of an international effort by the PRC government known as "Operation Fox Hunt" and "Operation Skynet."

In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges, rather than rely upon proper forms of international law enforcement cooperation.

Foreign investment reviews and telecommunications security

Beyond criminal enforcement, the Department worked to protect our national assets from national security risks posed by entities, subject to PRC influence, that seek to invest in U.S. companies or integrate into our supply chains.

In April, the Department assumed the permanent chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, established by the President through Executive Order (EO), in 2020. This organization, also known as "Team Telecom," is an interagency group that reviews telecommunications, submarine cable landing, wireless, broadcast license, and other applications referred by the Federal Communications Commission (FCC), to identify and address risks to national security and law enforcement. In the first 90 days after the Executive Order, the Department led Team Telecom to resolve more than half of the cases then pending review.

Team Telecom recommended that the FCC revoke and terminate the international telecommunications licenses held by the U.S. subsidiary of a PRC state-owned telecommunications company, China Telecom, the first revocation ever recommended by Team Telecom on national security grounds. Team Telecom

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a direct connection between the United States and Hong Kong.

Following the President's 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the Department has worked with the Commerce Department to develop regulations implementing the EO and has identified vulnerable areas of critical infrastructure that are ripe for investigation under the EO.

The Department also worked to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), which improved the authorities of the Committee on Foreign Investment in the United States (CFIUS). During the previous year, the Department co-led a record number of significant CFIUS matters, on an annualized basis, including the investigation of the acquisition of a U.S. hotel management software company by a Chinese company, which the President prohibited, for just the sixth time in CFIUS history. Under FIRRMA, the FBI continued to provide analytical assistance to support CFIUS's decision-making and identify high-risk non-notified transactions.

With its increased resources, NSD has played a significant role in CFIUS enforcement, leading the Committee to assess just the second penalty in its history, for failing to secure sensitive personal data in violation of a 2018 interim CFIUS order. NSD also dedicated personnel to identify transactions of concern that were not voluntarily filed with CFIUS and developed a program to identify bankruptcy cases that could implicate national security concerns. The bankruptcy program helps to protect U.S. assets from predatory acquisitions, including PRC acquisitions that could impact our national security, which is particularly important in light of the economic impact of COVID-19.

Education and outreach

The success of the China Initiative is not measured by criminal cases and administrative actions alone, however. Outreach to businesses and academia is critical to helping America's national assets better protect themselves. For that reason, the Department disseminated outreach presentations for use by U.S. Attorneys in their Districts, which have been deployed at various events. The FBI sustained its engagement with the private sector through various programs, and it developed and disseminated an innovative Academia Field Guide to support focused outreach by its academic outreach coordinators in all 56 field offices. In the coming year, the Department, through the FBI and U.S. Attorneys' Offices, will continue to expand our partnerships outside the federal government, because the support of the American people is critical to our success. All of our efforts are on their behalf.

The Attorney General commends the professionals throughout the Department, including those who work at Main Justice, the FBI, and U.S. Attorney's Offices around the country, who are committed to meeting the goals of the China Initiative and encourage them to redouble their efforts in the upcoming year.

All defendants, in the cases mentioned herein, are presumed innocent until proven guilty beyond a reasonable doubt.

###

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.

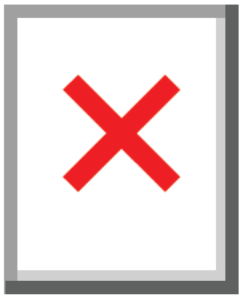
AG

20-1238

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.

Follow us:

From: USDOJ-Office of Public Affairs
Subject: THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)
To: Schreiber, Jayne (OAG)
Sent: November 16, 2020 11:27 AM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

MONDAY, NOVEMBER 16, 2020

THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)

WASHINGTON --- On the two-year anniversary of the Attorney General's China Initiative, the Department continues its significant focus on the Initiative's goals and announced substantial progress during the past year in disrupting and deterring the wide range of national security threats posed by the policies and practices of the People's Republic of China (PRC) government.

"In the last year, the Department has made incredible strides in countering the systemic efforts by the PRC to enhance its economic and military strength at America's expense," said Attorney General William P. Barr. "While much work remains to be done, the Department is committed to holding to account those who would steal, or otherwise illicitly obtain, the U.S. intellectual capital that will propel the future."

"The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt," said FBI Director Christopher Wray. "The FBI opens a new China-related counterintelligence case nearly every 10 hours and we'll continue our aggressive efforts to counter China's criminal activity."

Established in November 2018, the Initiative identified a number of goals for the Department, ranging from increased focus on the investigation and prosecution of trade secret theft and economic espionage, to better countering threats posed by Chinese foreign investment and supply chain vulnerabilities.

Prioritize investigations of economic espionage and trade secret theft

The Initiative prioritizes use of the Department's core tool, criminal investigation and prosecution, to counter economic espionage and other forms of trade secret theft. In the past year, the Department charged three economic espionage cases (in which the trade secret theft was intended to benefit the Chinese government), bringing the total to five since the China Initiative was first announced. Overall, since the Initiative was announced, we have charged more than 10 cases in which the trade secret theft had some alleged nexus to China, and we obtained guilty pleas of three defendants in those cases over the past year.

To take one example, the Department announced the China Initiative on the same day that it unsealed criminal charges against United Microelectronics (UMC), the Chinese state-owned enterprise Fujian Jinhua, and several individual defendants, for economic espionage that victimized Micron Technology, Inc., a leading U.S. semiconductor company.

"The United Microelectronics case is a glaring example of the PRC's 'rob, replicate, and replace' strategy, in which it robs a U.S. institution of its intellectual capital, replicates the stolen technology, and then endeavors to replace the U.S. institution on the Chinese and then the global market," said John Demers, Assistant Attorney General for National Security. "Thanks to the dedication and diligence of prosecutors and FBI agents, UMC pleaded guilty to criminal trade secret theft and agreed to pay a fine of $60 million, the second largest fine in a trade secret case, and to cooperate in the pending prosecution of its co-defendants."

The National Counterintelligence Task Force, co-led by the FBI, launched its first major campaign in 2020, devoted to protecting U.S. technology and research from the Chinese government and its proxies. This is a further step in the FBI's and Department's efforts to enlist all appropriate partners in ensuring integrity in government-funded programs and defeating economic espionage and theft of trade secrets.

Develop an enforcement strategy for non-traditional collectors

At the outset, the Department identified academia as one of our most vulnerable sectors, because its traditions of openness, and the importance of international exchanges to the free flow of ideas, leave it vulnerable to PRC exploitation. The Department has pursued a two-pronged strategy of raising awareness on campuses of the threats posed by China (and the importance of implementing a security program to detect them) and prosecuting researchers who have deliberately deceived authorities about their ties to China, which deprives institutions of the ability to screen for conflicts of interest and commitment, or otherwise exploited their access.

For example, the PRC has used talent programs to encourage the transfer of technical expertise from the United States, and elsewhere in the world, to benefit the PRC's economic and military development. Talent recruits generally sign contracts with the PRC sponsor-entity that obligate them to produce scientific outputs; to publish the results of their work in the name of the PRC beneficiary; to allow the PRC beneficiary to assert intellectual property rights over their outputs; and to recruit other researchers into the programs, among other obligations.

In exchange, the talent recruits may receive lucrative compensation packages, prestigious titles, and custom-built laboratories.

"While membership in these talent programs is not *per se* illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to

work in the interest of the Chinese Communist Party," said Adam S. Hickey, Deputy Assistant Attorney General, National Security Division.

The Initiative brings together resources from across the Department, including the National Security, Criminal, Tax, and the Civil Divisions to address this unique challenge fairly and effectively. In the past year, Department prosecutors have brought fraud, false statements, tax, smuggling and other charges against ten academics affiliated with research institutions across the country. To date, prosecutors have obtained convictions in three of those cases.

This year, the FBI and Department prosecutors also exposed six individuals, studying in the United States, found to be connected to People's Liberation Army military institutes, who concealed their affiliations from the State Department when applying for research visas to study at U.S. universities. In one of those cases, the Department alleged that a PLA officer was being tasked by superiors in the PRC to obtain information that would benefit PLA operations. In another case, a PLA medical researcher stands accused of following orders to observe lab operations at a U.S. university, which received funding from the U.S. government, in order to replicate those operations in the PRC.

In each of the cases, the defendants are accused of concealing their PLA affiliations in order to obtain visas that allowed them to travel to the United States. After the FBI conducted interviews this summer that led to charges in those cases and the State Department closed the PRC's Houston Consulate, a large number of undeclared, PLA-affiliated Chinese researchers fled the United States.

Those six examples are just part of the interagency effort to protect academia and taxpayer-funded research. The FBI and Department have been collaborating with federal grant-making agencies, the Joint Committee on the Research Environment, the major academic associations, the Academic Security and Counter Exploitation working group, and other appropriate entities, as well as hundreds of individual universities nationwide.

Counter malicious cyber activity

The Department continues to expose and disrupt efforts by the PRC government to steal our intellectual property and our personally identifiable information (PII) through computer intrusions. During the past year, we charged hackers working for the People's Liberation Army with the 2017 Equifax intrusion and others associated with the Ministry of State Security (MSS) in relation to global computer intrusion campaigns targeting biomedical companies conducting COVID-19-related research, engineering firms, and software makers. One such MSS case resulted in the arrest of two conspirators in Malaysia. Two of these cases highlighted China's development into a safe harbor for criminal hackers who also work for the PRC. The Department disrupted these cyber threats in coordination with the private sector, using legal process to seize control of hacking infrastructure while the private sector removed other infrastructure from their platforms.

In May, the FBI, in conjunction with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, also issued a public announcement to raise awareness of the threat to COVID-19 research by PRC-affiliated cyber actors and offer advice on better protecting that research from thefts.

Counter malign foreign influence

The Department has used the Foreign Agents Registration Act ("FARA"), which requires those acting to influence public policy and opinion on behalf of a foreign individual or entity, to improve transparency and expose China's foreign influence efforts. Over the past year, the Department opened a record number of FARA investigations overall and doubled the number of new registrants and new foreign principals registering annually as of 2016. That includes obtaining a record number of registrations from Chinese media companies. The Department also notified a registered Chinese media company that its filings were deficient because they failed to fully disclose its activity in the United States and failed to properly label its informational materials. The media entity remedied those deficiencies shortly thereafter.

Through its outreach efforts to universities, the Department has highlighted the need to protect foreign students studying in the United States from coercive efforts by the Communist Party to censor the freedom of thought and expression that all students here should enjoy.

In late 2019, the FBI's Foreign Influence Task Force formally established a new unit devoted specifically

to understanding and defeating the malign foreign influence threat from the Chinese government and its proxies.

Counter foreign intelligence activities

The Department has achieved a number of successes in the last year in countering China's foreign intelligence activities. China has been targeting former members of the U.S. intelligence community for recruitment, and the Department has been holding accountable individuals who succumb to their efforts. In November 2019, a former CIA case officer was sentenced to 19 years in prison for conspiring to deliver national defense information to the PRC. In August 2020, another former CIA officer who had been tasked by the PRC was arrested on the same charge — the fourth former intelligence officer charged in the last three years for similar conduct.

The Department is particularly focused on disrupting the PRC government from using career networking and social media sites to target Americans, as well as holding those accountable who hide behind fake profiles to co-opt individuals on behalf of the PRC. As one part of this effort, the FBI, in partnership with the National Counterintelligence and Security Center, created an educational film, "The Nevernight Connection," which was released online in September 2020 to educate the public about the Chinese intelligence services' use of social media to spot and recruit persons of interest, especially current or former security clearance holders.

In March 2020, Xuehua (Edward) Peng was sentenced to 48 months in prison, and ordered to pay a $30,000 fine, for acting as an agent of the PRC's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital cards containing classified information from a source in the United States to the MSS operatives in China.

In October 2020, Jun Wei Yeo was sentenced to 14 months in prison for acting within the United States as an agent of the MSS recruiting Americans, including U.S. military and government employees with high-level clearances. Yeo concealed his MSS affiliation from his American targets and used career networking sites and a false consulting firm to lure them to write papers which he ultimately passed to his MSS handlers.

In October 2020, eight defendants were charged with conspiring to act in the United States as illegal agents of the PRC, six of whom also face related charges of conspiring to commit interstate and international stalking. According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate a resident of New Jersey and his family in order to force them to return to the PRC as part of an international effort by the PRC government known as "Operation Fox Hunt" and "Operation Skynet."

In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges, rather than rely upon proper forms of international law enforcement cooperation.

Foreign investment reviews and telecommunications security

Beyond criminal enforcement, the Department worked to protect our national assets from national security risks posed by entities, subject to PRC influence, that seek to invest in U.S. companies or integrate into our supply chains.

In April, the Department assumed the permanent chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, established by the President through Executive Order (EO), in 2020. This organization, also known as "Team Telecom," is an interagency group that reviews telecommunications, submarine cable landing, wireless, broadcast license, and other applications referred by the Federal Communications Commission (FCC), to identify and address risks to national security and law enforcement. In the first 90 days after the Executive Order, the Department led Team Telecom to resolve more than half of the cases then pending review.

Team Telecom recommended that the FCC revoke and terminate the international telecommunications licenses held by the U.S. subsidiary of a PRC state-owned telecommunications company, China Telecom, the first revocation ever recommended by Team Telecom on national security grounds. Team Telecom

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a direct connection between the United States and Hong Kong.

Following the President's 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the Department has worked with the Commerce Department to develop regulations implementing the EO and has identified vulnerable areas of critical infrastructure that are ripe for investigation under the EO.

The Department also worked to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), which improved the authorities of the Committee on Foreign Investment in the United States (CFIUS). During the previous year, the Department co-led a record number of significant CFIUS matters, on an annualized basis, including the investigation of the acquisition of a U.S. hotel management software company by a Chinese company, which the President prohibited, for just the sixth time in CFIUS history. Under FIRRMA, the FBI continued to provide analytical assistance to support CFIUS's decision-making and identify high-risk non-notified transactions.

With its increased resources, NSD has played a significant role in CFIUS enforcement, leading the Committee to assess just the second penalty in its history, for failing to secure sensitive personal data in violation of a 2018 interim CFIUS order. NSD also dedicated personnel to identify transactions of concern that were not voluntarily filed with CFIUS and developed a program to identify bankruptcy cases that could implicate national security concerns. The bankruptcy program helps to protect U.S. assets from predatory acquisitions, including PRC acquisitions that could impact our national security, which is particularly important in light of the economic impact of COVID-19.

Education and outreach

The success of the China Initiative is not measured by criminal cases and administrative actions alone, however. Outreach to businesses and academia is critical to helping America's national assets better protect themselves. For that reason, the Department disseminated outreach presentations for use by U.S. Attorneys in their Districts, which have been deployed at various events. The FBI sustained its engagement with the private sector through various programs, and it developed and disseminated an innovative Academia Field Guide to support focused outreach by its academic outreach coordinators in all 56 field offices. In the coming year, the Department, through the FBI and U.S. Attorneys' Offices, will continue to expand our partnerships outside the federal government, because the support of the American people is critical to our success. All of our efforts are on their behalf.

The Attorney General commends the professionals throughout the Department, including those who work at Main Justice, the FBI, and U.S. Attorney's Offices around the country, who are committed to meeting the goals of the China Initiative and encourage them to redouble their efforts in the upcoming year.

All defendants, in the cases mentioned herein, are presumed innocent until proven guilty beyond a reasonable doubt.

###

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.

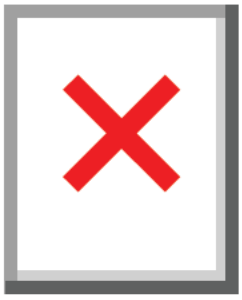
AG

20-1238

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.

Follow us:

From: USDOJ-Office of Public Affairs
Subject: THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)
To: Levi, William (OAG)
Sent: November 16, 2020 11:27 AM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

MONDAY, NOVEMBER 16, 2020

THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)

WASHINGTON --- On the two-year anniversary of the Attorney General's China Initiative, the Department continues its significant focus on the Initiative's goals and announced substantial progress during the past year in disrupting and deterring the wide range of national security threats posed by the policies and practices of the People's Republic of China (PRC) government.

"In the last year, the Department has made incredible strides in countering the systemic efforts by the PRC to enhance its economic and military strength at America's expense," said Attorney General William P. Barr. "While much work remains to be done, the Department is committed to holding to account those who would steal, or otherwise illicitly obtain, the U.S. intellectual capital that will propel the future."

"The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt," said FBI Director Christopher Wray. "The FBI opens a new China-related counterintelligence case nearly every 10 hours and we'll continue our aggressive efforts to counter China's criminal activity."

Established in November 2018, the Initiative identified a number of goals for the Department, ranging from increased focus on the investigation and prosecution of trade secret theft and economic espionage, to better countering threats posed by Chinese foreign investment and supply chain vulnerabilities.

Prioritize investigations of economic espionage and trade secret theft

The Initiative prioritizes use of the Department's core tool, criminal investigation and prosecution, to counter economic espionage and other forms of trade secret theft. In the past year, the Department charged three economic espionage cases (in which the trade secret theft was intended to benefit the Chinese government), bringing the total to five since the China Initiative was first announced. Overall, since the Initiative was announced, we have charged more than 10 cases in which the trade secret theft had some alleged nexus to China, and we obtained guilty pleas of three defendants in those cases over the past year.

To take one example, the Department announced the China Initiative on the same day that it unsealed criminal charges against United Microelectronics (UMC), the Chinese state-owned enterprise Fujian Jinhua, and several individual defendants, for economic espionage that victimized Micron Technology, Inc., a leading U.S. semiconductor company.

"The United Microelectronics case is a glaring example of the PRC's 'rob, replicate, and replace' strategy, in which it robs a U.S. institution of its intellectual capital, replicates the stolen technology, and then endeavors to replace the U.S. institution on the Chinese and then the global market," said John Demers, Assistant Attorney General for National Security. "Thanks to the dedication and diligence of prosecutors and FBI agents, UMC pleaded guilty to criminal trade secret theft and agreed to pay a fine of $60 million, the second largest fine in a trade secret case, and to cooperate in the pending prosecution of its co-defendants."

The National Counterintelligence Task Force, co-led by the FBI, launched its first major campaign in 2020, devoted to protecting U.S. technology and research from the Chinese government and its proxies. This is a further step in the FBI's and Department's efforts to enlist all appropriate partners in ensuring integrity in government-funded programs and defeating economic espionage and theft of trade secrets.

Develop an enforcement strategy for non-traditional collectors

At the outset, the Department identified academia as one of our most vulnerable sectors, because its traditions of openness, and the importance of international exchanges to the free flow of ideas, leave it vulnerable to PRC exploitation. The Department has pursued a two-pronged strategy of raising awareness on campuses of the threats posed by China (and the importance of implementing a security program to detect them) and prosecuting researchers who have deliberately deceived authorities about their ties to China, which deprives institutions of the ability to screen for conflicts of interest and commitment, or otherwise exploited their access.

For example, the PRC has used talent programs to encourage the transfer of technical expertise from the United States, and elsewhere in the world, to benefit the PRC's economic and military development. Talent recruits generally sign contracts with the PRC sponsor-entity that obligate them to produce scientific outputs; to publish the results of their work in the name of the PRC beneficiary; to allow the PRC beneficiary to assert intellectual property rights over their outputs; and to recruit other researchers into the programs, among other obligations.

In exchange, the talent recruits may receive lucrative compensation packages, prestigious titles, and custom-built laboratories.

"While membership in these talent programs is not *per se* illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to

work in the interest of the Chinese Communist Party," said Adam S. Hickey, Deputy Assistant Attorney General, National Security Division.

The Initiative brings together resources from across the Department, including the National Security, Criminal, Tax, and the Civil Divisions to address this unique challenge fairly and effectively. In the past year, Department prosecutors have brought fraud, false statements, tax, smuggling and other charges against ten academics affiliated with research institutions across the country. To date, prosecutors have obtained convictions in three of those cases.

This year, the FBI and Department prosecutors also exposed six individuals, studying in the United States, found to be connected to People's Liberation Army military institutes, who concealed their affiliations from the State Department when applying for research visas to study at U.S. universities. In one of those cases, the Department alleged that a PLA officer was being tasked by superiors in the PRC to obtain information that would benefit PLA operations. In another case, a PLA medical researcher stands accused of following orders to observe lab operations at a U.S. university, which received funding from the U.S. government, in order to replicate those operations in the PRC.

In each of the cases, the defendants are accused of concealing their PLA affiliations in order to obtain visas that allowed them to travel to the United States. After the FBI conducted interviews this summer that led to charges in those cases and the State Department closed the PRC's Houston Consulate, a large number of undeclared, PLA-affiliated Chinese researchers fled the United States.

Those six examples are just part of the interagency effort to protect academia and taxpayer-funded research. The FBI and Department have been collaborating with federal grant-making agencies, the Joint Committee on the Research Environment, the major academic associations, the Academic Security and Counter Exploitation working group, and other appropriate entities, as well as hundreds of individual universities nationwide.

Counter malicious cyber activity

The Department continues to expose and disrupt efforts by the PRC government to steal our intellectual property and our personally identifiable information (PII) through computer intrusions. During the past year, we charged hackers working for the People's Liberation Army with the 2017 Equifax intrusion and others associated with the Ministry of State Security (MSS) in relation to global computer intrusion campaigns targeting biomedical companies conducting COVID-19-related research, engineering firms, and software makers. One such MSS case resulted in the arrest of two conspirators in Malaysia. Two of these cases highlighted China's development into a safe harbor for criminal hackers who also work for the PRC. The Department disrupted these cyber threats in coordination with the private sector, using legal process to seize control of hacking infrastructure while the private sector removed other infrastructure from their platforms.

In May, the FBI, in conjunction with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, also issued a public announcement to raise awareness of the threat to COVID-19 research by PRC-affiliated cyber actors and offer advice on better protecting that research from thefts.

Counter malign foreign influence

The Department has used the Foreign Agents Registration Act ("FARA"), which requires those acting to influence public policy and opinion on behalf of a foreign individual or entity, to improve transparency and expose China's foreign influence efforts. Over the past year, the Department opened a record number of FARA investigations overall and doubled the number of new registrants and new foreign principals registering annually as of 2016. That includes obtaining a record number of registrations from Chinese media companies. The Department also notified a registered Chinese media company that its filings were deficient because they failed to fully disclose its activity in the United States and failed to properly label its informational materials. The media entity remedied those deficiencies shortly thereafter.

Through its outreach efforts to universities, the Department has highlighted the need to protect foreign students studying in the United States from coercive efforts by the Communist Party to censor the freedom of thought and expression that all students here should enjoy.

In late 2019, the FBI's Foreign Influence Task Force formally established a new unit devoted specifically

to understanding and defeating the malign foreign influence threat from the Chinese government and its proxies.

Counter foreign intelligence activities

The Department has achieved a number of successes in the last year in countering China's foreign intelligence activities. China has been targeting former members of the U.S. intelligence community for recruitment, and the Department has been holding accountable individuals who succumb to their efforts. In November 2019, a former CIA case officer was sentenced to 19 years in prison for conspiring to deliver national defense information to the PRC. In August 2020, another former CIA officer who had been tasked by the PRC was arrested on the same charge — the fourth former intelligence officer charged in the last three years for similar conduct.

The Department is particularly focused on disrupting the PRC government from using career networking and social media sites to target Americans, as well as holding those accountable who hide behind fake profiles to co-opt individuals on behalf of the PRC. As one part of this effort, the FBI, in partnership with the National Counterintelligence and Security Center, created an educational film, "The Nevernight Connection," which was released online in September 2020 to educate the public about the Chinese intelligence services' use of social media to spot and recruit persons of interest, especially current or former security clearance holders.

In March 2020, Xuehua (Edward) Peng was sentenced to 48 months in prison, and ordered to pay a $30,000 fine, for acting as an agent of the PRC's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital cards containing classified information from a source in the United States to the MSS operatives in China.

In October 2020, Jun Wei Yeo was sentenced to 14 months in prison for acting within the United States as an agent of the MSS recruiting Americans, including U.S. military and government employees with high-level clearances. Yeo concealed his MSS affiliation from his American targets and used career networking sites and a false consulting firm to lure them to write papers which he ultimately passed to his MSS handlers.

In October 2020, eight defendants were charged with conspiring to act in the United States as illegal agents of the PRC, six of whom also face related charges of conspiring to commit interstate and international stalking. According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate a resident of New Jersey and his family in order to force them to return to the PRC as part of an international effort by the PRC government known as "Operation Fox Hunt" and "Operation Skynet."

In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges, rather than rely upon proper forms of international law enforcement cooperation.

Foreign investment reviews and telecommunications security

Beyond criminal enforcement, the Department worked to protect our national assets from national security risks posed by entities, subject to PRC influence, that seek to invest in U.S. companies or integrate into our supply chains.

In April, the Department assumed the permanent chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, established by the President through Executive Order (EO), in 2020. This organization, also known as "Team Telecom," is an interagency group that reviews telecommunications, submarine cable landing, wireless, broadcast license, and other applications referred by the Federal Communications Commission (FCC), to identify and address risks to national security and law enforcement. In the first 90 days after the Executive Order, the Department led Team Telecom to resolve more than half of the cases then pending review.

Team Telecom recommended that the FCC revoke and terminate the international telecommunications licenses held by the U.S. subsidiary of a PRC state-owned telecommunications company, China Telecom, the first revocation ever recommended by Team Telecom on national security grounds. Team Telecom

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a direct connection between the United States and Hong Kong.

Following the President's 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the Department has worked with the Commerce Department to develop regulations implementing the EO and has identified vulnerable areas of critical infrastructure that are ripe for investigation under the EO.

The Department also worked to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), which improved the authorities of the Committee on Foreign Investment in the United States (CFIUS). During the previous year, the Department co-led a record number of significant CFIUS matters, on an annualized basis, including the investigation of the acquisition of a U.S. hotel management software company by a Chinese company, which the President prohibited, for just the sixth time in CFIUS history. Under FIRRMA, the FBI continued to provide analytical assistance to support CFIUS's decision-making and identify high-risk non-notified transactions.

With its increased resources, NSD has played a significant role in CFIUS enforcement, leading the Committee to assess just the second penalty in its history, for failing to secure sensitive personal data in violation of a 2018 interim CFIUS order. NSD also dedicated personnel to identify transactions of concern that were not voluntarily filed with CFIUS and developed a program to identify bankruptcy cases that could implicate national security concerns. The bankruptcy program helps to protect U.S. assets from predatory acquisitions, including PRC acquisitions that could impact our national security, which is particularly important in light of the economic impact of COVID-19.

Education and outreach

The success of the China Initiative is not measured by criminal cases and administrative actions alone, however. Outreach to businesses and academia is critical to helping America's national assets better protect themselves. For that reason, the Department disseminated outreach presentations for use by U.S. Attorneys in their Districts, which have been deployed at various events. The FBI sustained its engagement with the private sector through various programs, and it developed and disseminated an innovative Academia Field Guide to support focused outreach by its academic outreach coordinators in all 56 field offices. In the coming year, the Department, through the FBI and U.S. Attorneys' Offices, will continue to expand our partnerships outside the federal government, because the support of the American people is critical to our success. All of our efforts are on their behalf.

The Attorney General commends the professionals throughout the Department, including those who work at Main Justice, the FBI, and U.S. Attorney's Offices around the country, who are committed to meeting the goals of the China Initiative and encourage them to redouble their efforts in the upcoming year.

All defendants, in the cases mentioned herein, are presumed innocent until proven guilty beyond a reasonable doubt.

###

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.

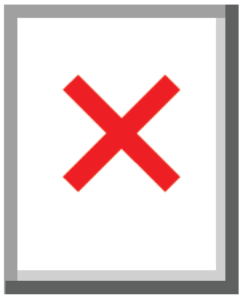
AG

20-1238

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.

Follow us:

From: USDOJ-Office of Public Affairs
Subject: THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)
To: Watson, Theresa (OAG)
Sent: November 16, 2020 11:27 AM (UTC-05:00)



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

MONDAY, NOVEMBER 16, 2020

THE CHINA INITIATIVE: YEAR-IN-REVIEW (2019-20)

WASHINGTON --- On the two-year anniversary of the Attorney General's China Initiative, the Department continues its significant focus on the Initiative's goals and announced substantial progress during the past year in disrupting and deterring the wide range of national security threats posed by the policies and practices of the People's Republic of China (PRC) government.

"In the last year, the Department has made incredible strides in countering the systemic efforts by the PRC to enhance its economic and military strength at America's expense," said Attorney General William P. Barr. "While much work remains to be done, the Department is committed to holding to account those who would steal, or otherwise illicitly obtain, the U.S. intellectual capital that will propel the future."

"The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt," said FBI Director Christopher Wray. "The FBI opens a new China-related counterintelligence case nearly every 10 hours and we'll continue our aggressive efforts to counter China's criminal activity."

Established in November 2018, the Initiative identified a number of goals for the Department, ranging from increased focus on the investigation and prosecution of trade secret theft and economic espionage, to better countering threats posed by Chinese foreign investment and supply chain vulnerabilities.

Prioritize investigations of economic espionage and trade secret theft

The Initiative prioritizes use of the Department's core tool, criminal investigation and prosecution, to counter economic espionage and other forms of trade secret theft. In the past year, the Department charged three economic espionage cases (in which the trade secret theft was intended to benefit the Chinese government), bringing the total to five since the China Initiative was first announced. Overall, since the Initiative was announced, we have charged more than 10 cases in which the trade secret theft had some alleged nexus to China, and we obtained guilty pleas of three defendants in those cases over the past year.

To take one example, the Department announced the China Initiative on the same day that it unsealed criminal charges against United Microelectronics (UMC), the Chinese state-owned enterprise Fujian Jinhua, and several individual defendants, for economic espionage that victimized Micron Technology, Inc., a leading U.S. semiconductor company.

"The United Microelectronics case is a glaring example of the PRC's 'rob, replicate, and replace' strategy, in which it robs a U.S. institution of its intellectual capital, replicates the stolen technology, and then endeavors to replace the U.S. institution on the Chinese and then the global market," said John Demers, Assistant Attorney General for National Security. "Thanks to the dedication and diligence of prosecutors and FBI agents, UMC pleaded guilty to criminal trade secret theft and agreed to pay a fine of $60 million, the second largest fine in a trade secret case, and to cooperate in the pending prosecution of its co-defendants."

The National Counterintelligence Task Force, co-led by the FBI, launched its first major campaign in 2020, devoted to protecting U.S. technology and research from the Chinese government and its proxies. This is a further step in the FBI's and Department's efforts to enlist all appropriate partners in ensuring integrity in government-funded programs and defeating economic espionage and theft of trade secrets.

Develop an enforcement strategy for non-traditional collectors

At the outset, the Department identified academia as one of our most vulnerable sectors, because its traditions of openness, and the importance of international exchanges to the free flow of ideas, leave it vulnerable to PRC exploitation. The Department has pursued a two-pronged strategy of raising awareness on campuses of the threats posed by China (and the importance of implementing a security program to detect them) and prosecuting researchers who have deliberately deceived authorities about their ties to China, which deprives institutions of the ability to screen for conflicts of interest and commitment, or otherwise exploited their access.

For example, the PRC has used talent programs to encourage the transfer of technical expertise from the United States, and elsewhere in the world, to benefit the PRC's economic and military development. Talent recruits generally sign contracts with the PRC sponsor-entity that obligate them to produce scientific outputs; to publish the results of their work in the name of the PRC beneficiary; to allow the PRC beneficiary to assert intellectual property rights over their outputs; and to recruit other researchers into the programs, among other obligations.

In exchange, the talent recruits may receive lucrative compensation packages, prestigious titles, and custom-built laboratories.

"While membership in these talent programs is not *per se* illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to

work in the interest of the Chinese Communist Party," said Adam S. Hickey, Deputy Assistant Attorney General, National Security Division.

The Initiative brings together resources from across the Department, including the National Security, Criminal, Tax, and the Civil Divisions to address this unique challenge fairly and effectively. In the past year, Department prosecutors have brought fraud, false statements, tax, smuggling and other charges against ten academics affiliated with research institutions across the country. To date, prosecutors have obtained convictions in three of those cases.

This year, the FBI and Department prosecutors also exposed six individuals, studying in the United States, found to be connected to People's Liberation Army military institutes, who concealed their affiliations from the State Department when applying for research visas to study at U.S. universities. In one of those cases, the Department alleged that a PLA officer was being tasked by superiors in the PRC to obtain information that would benefit PLA operations. In another case, a PLA medical researcher stands accused of following orders to observe lab operations at a U.S. university, which received funding from the U.S. government, in order to replicate those operations in the PRC.

In each of the cases, the defendants are accused of concealing their PLA affiliations in order to obtain visas that allowed them to travel to the United States. After the FBI conducted interviews this summer that led to charges in those cases and the State Department closed the PRC's Houston Consulate, a large number of undeclared, PLA-affiliated Chinese researchers fled the United States.

Those six examples are just part of the interagency effort to protect academia and taxpayer-funded research. The FBI and Department have been collaborating with federal grant-making agencies, the Joint Committee on the Research Environment, the major academic associations, the Academic Security and Counter Exploitation working group, and other appropriate entities, as well as hundreds of individual universities nationwide.

Counter malicious cyber activity

The Department continues to expose and disrupt efforts by the PRC government to steal our intellectual property and our personally identifiable information (PII) through computer intrusions. During the past year, we charged hackers working for the People's Liberation Army with the 2017 Equifax intrusion and others associated with the Ministry of State Security (MSS) in relation to global computer intrusion campaigns targeting biomedical companies conducting COVID-19-related research, engineering firms, and software makers. One such MSS case resulted in the arrest of two conspirators in Malaysia. Two of these cases highlighted China's development into a safe harbor for criminal hackers who also work for the PRC. The Department disrupted these cyber threats in coordination with the private sector, using legal process to seize control of hacking infrastructure while the private sector removed other infrastructure from their platforms.

In May, the FBI, in conjunction with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, also issued a public announcement to raise awareness of the threat to COVID-19 research by PRC-affiliated cyber actors and offer advice on better protecting that research from thefts.

Counter malign foreign influence

The Department has used the Foreign Agents Registration Act ("FARA"), which requires those acting to influence public policy and opinion on behalf of a foreign individual or entity, to improve transparency and expose China's foreign influence efforts. Over the past year, the Department opened a record number of FARA investigations overall and doubled the number of new registrants and new foreign principals registering annually as of 2016. That includes obtaining a record number of registrations from Chinese media companies. The Department also notified a registered Chinese media company that its filings were deficient because they failed to fully disclose its activity in the United States and failed to properly label its informational materials. The media entity remedied those deficiencies shortly thereafter.

Through its outreach efforts to universities, the Department has highlighted the need to protect foreign students studying in the United States from coercive efforts by the Communist Party to censor the freedom of thought and expression that all students here should enjoy.

In late 2019, the FBI's Foreign Influence Task Force formally established a new unit devoted specifically

to understanding and defeating the malign foreign influence threat from the Chinese government and its proxies.

Counter foreign intelligence activities

The Department has achieved a number of successes in the last year in countering China's foreign intelligence activities. China has been targeting former members of the U.S. intelligence community for recruitment, and the Department has been holding accountable individuals who succumb to their efforts. In November 2019, a former CIA case officer was sentenced to 19 years in prison for conspiring to deliver national defense information to the PRC. In August 2020, another former CIA officer who had been tasked by the PRC was arrested on the same charge — the fourth former intelligence officer charged in the last three years for similar conduct.

The Department is particularly focused on disrupting the PRC government from using career networking and social media sites to target Americans, as well as holding those accountable who hide behind fake profiles to co-opt individuals on behalf of the PRC. As one part of this effort, the FBI, in partnership with the National Counterintelligence and Security Center, created an educational film, "The Nevernight Connection," which was released online in September 2020 to educate the public about the Chinese intelligence services' use of social media to spot and recruit persons of interest, especially current or former security clearance holders.

In March 2020, Xuehua (Edward) Peng was sentenced to 48 months in prison, and ordered to pay a $30,000 fine, for acting as an agent of the PRC's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital cards containing classified information from a source in the United States to the MSS operatives in China.

In October 2020, Jun Wei Yeo was sentenced to 14 months in prison for acting within the United States as an agent of the MSS recruiting Americans, including U.S. military and government employees with high-level clearances. Yeo concealed his MSS affiliation from his American targets and used career networking sites and a false consulting firm to lure them to write papers which he ultimately passed to his MSS handlers.

In October 2020, eight defendants were charged with conspiring to act in the United States as illegal agents of the PRC, six of whom also face related charges of conspiring to commit interstate and international stalking. According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate a resident of New Jersey and his family in order to force them to return to the PRC as part of an international effort by the PRC government known as "Operation Fox Hunt" and "Operation Skynet."

In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges, rather than rely upon proper forms of international law enforcement cooperation.

Foreign investment reviews and telecommunications security

Beyond criminal enforcement, the Department worked to protect our national assets from national security risks posed by entities, subject to PRC influence, that seek to invest in U.S. companies or integrate into our supply chains.

In April, the Department assumed the permanent chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, established by the President through Executive Order (EO), in 2020. This organization, also known as "Team Telecom," is an interagency group that reviews telecommunications, submarine cable landing, wireless, broadcast license, and other applications referred by the Federal Communications Commission (FCC), to identify and address risks to national security and law enforcement. In the first 90 days after the Executive Order, the Department led Team Telecom to resolve more than half of the cases then pending review.

Team Telecom recommended that the FCC revoke and terminate the international telecommunications licenses held by the U.S. subsidiary of a PRC state-owned telecommunications company, China Telecom, the first revocation ever recommended by Team Telecom on national security grounds. Team Telecom

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a

also recommended that the FCC partially deny a submarine cable application, to the extent it sought a direct connection between the United States and Hong Kong.

Following the President's 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the Department has worked with the Commerce Department to develop regulations implementing the EO and has identified vulnerable areas of critical infrastructure that are ripe for investigation under the EO.

The Department also worked to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), which improved the authorities of the Committee on Foreign Investment in the United States (CFIUS). During the previous year, the Department co-led a record number of significant CFIUS matters, on an annualized basis, including the investigation of the acquisition of a U.S. hotel management software company by a Chinese company, which the President prohibited, for just the sixth time in CFIUS history. Under FIRRMA, the FBI continued to provide analytical assistance to support CFIUS's decision-making and identify high-risk non-notified transactions.

With its increased resources, NSD has played a significant role in CFIUS enforcement, leading the Committee to assess just the second penalty in its history, for failing to secure sensitive personal data in violation of a 2018 interim CFIUS order. NSD also dedicated personnel to identify transactions of concern that were not voluntarily filed with CFIUS and developed a program to identify bankruptcy cases that could implicate national security concerns. The bankruptcy program helps to protect U.S. assets from predatory acquisitions, including PRC acquisitions that could impact our national security, which is particularly important in light of the economic impact of COVID-19.

Education and outreach

The success of the China Initiative is not measured by criminal cases and administrative actions alone, however. Outreach to businesses and academia is critical to helping America's national assets better protect themselves. For that reason, the Department disseminated outreach presentations for use by U.S. Attorneys in their Districts, which have been deployed at various events. The FBI sustained its engagement with the private sector through various programs, and it developed and disseminated an innovative Academia Field Guide to support focused outreach by its academic outreach coordinators in all 56 field offices. In the coming year, the Department, through the FBI and U.S. Attorneys' Offices, will continue to expand our partnerships outside the federal government, because the support of the American people is critical to our success. All of our efforts are on their behalf.

The Attorney General commends the professionals throughout the Department, including those who work at Main Justice, the FBI, and U.S. Attorney's Offices around the country, who are committed to meeting the goals of the China Initiative and encourage them to redouble their efforts in the upcoming year.

All defendants, in the cases mentioned herein, are presumed innocent until proven guilty beyond a reasonable doubt.

###

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.

AG

20-1238

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.

Follow us:

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: Bryant, Errical (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: Bissex, Rachel (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: Hamilton, Gene (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.