Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM April 2, 2019

To: Senate Finance Committee [redacted]

From: Wayne M. Morrison, Specialist in Asian Trade and Finance [redacted]

Subject: **China's Compliance with Certain Commitments on Intellectual Property**

This memorandum responds to your request for information regarding China's history of compliance with certain commitments it has made in the past on forced technology transfer and cyber-theft of U.S. trade secrets. These are two of the four issues that are being addressed in the current U.S. Section 301 investigation (initiated in August 2017) of "China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," and they are included in current negotiations between the United States and China.[1] Do not hesitate to contact me if I can be of additional assistance.[2]

On March 22, 2018, the U.S. Trade Representative (USTR) issued a report on its findings of the issues involved in the Section 301 investigation.[3] On China's forced technology and cyber-theft conduct, it concluded that:

- China uses foreign ownership restrictions, including joint venture requirements, equity limitations, and other investment restrictions, to require or pressure technology transfer from U.S. companies to Chinese entities. China also uses administrative review and licensing procedures to require or pressure technology transfer, which, inter alia, undermines the value of U.S. investments and technology and weakens the global competitiveness of U.S. firms.
- China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies. These actions provide the Chinese government with unauthorized access to intellectual property (IP), trade secrets, or confidential business information, including technical data, negotiating positions, and sensitive and proprietary internal business communications, and they also support China's strategic development

---

[1] For additional information on the Section 301 case against China, see CRS In Focus IF10708, *Enforcing U.S. Trade Laws: Section 301 and China*, by Wayne M. Morrison

[2] Information in this memorandum may be used in other CRS products.

[3] USTR, Press Release, March 22, 2018, available at https://ustr.gov/about-us/policy-offices/press-office/pressreleases/2018/march/president-trump-announces-strong.

goals, including its science and technology advancement, military modernization, and economic development.[4]

Forced Technology Transfer

China joined the World Trade Organization (WTO) in 2001. Under the terms of its accession, China pledged that:

> Without prejudice to the relevant provisions of this Protocol, China shall ensure that the distribution of import licenses, quotas, tariff-rate quotas, or any other means of approval for importation, the right of importation or investment by national and sub-national authorities, is not conditioned on: whether competing domestic suppliers of such products exist; or performance requirements of any kind, such as local content, offsets, the *transfer of technology*, export performance or the conduct of research and development in China.[5]

Further, the WTO's Working Party report on China's accession included a pledge from the Chinese government on technology transfer:

> Certain members of the Working Party expressed concern about laws, regulations and measures in China affecting the transfer of technology, in particular in the context of investment decisions. Moreover, these members expressed concern about measures conditioning the receipt of benefits, including investment approvals, upon technology transfer. In their view, the terms and conditions of technology transfer, particularly in the context of an investment, should be agreed between the parties to the investment without government interference. The government should not, for example, condition investment approval upon technology transfer.
>
> The representative of China confirmed that China would only impose, apply or enforce laws, regulations or measures relating to the transfer of technology, production processes, or other proprietary knowledge to an individual or enterprise in its territory that were not inconsistent with the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement") and the Agreement on Trade-Related Investment Measures ("TRIMs Agreement"). He confirmed that the terms and conditions of technology transfer, production processes or other proprietary knowledge, particularly in the context of an investment, would only require agreement between the parties to the investment. The Working Party took note of these commitments.[6]

Each year since 2002, the USTR has issued an annual report evaluating China's implementation of its WTO commitments. Every report has cited U.S. concern over forced technology transfer issues.[6] For example the 2002 report stated:

> Beginning before its accession to the WTO, China revised its laws and regulations on foreign invested enterprises to eliminate WTO-inconsistent requirements relating to export performance, local content and foreign exchange balancing as well as technology transfer. However, the revised laws and regulations continue to "encourage" technology transfer, without formally requiring it.

[4] The other two practices that the USTR found to be of concern were China's discriminatory technology licensing policies and China's efforts to obtain U.S. cutting-edge technology and IP through acquisitions of certain U.S. firms in order to advance its industrial policies, such as the Made in China 2025 plan. Although the USTR links all four practices to technology transfer, this memorandum examines those practices that have been subject to agreements between the United States and China.

[5] WTO, *Accession of the People's Republic of China, Decision of 10 November 2001*, November 23, 2001, p.5. [6]

WTO, *Working Party on the Accession of China*, October 1, 2001, p. 9.

[6] The United States has not sought to use the WTO Dispute Settlement system to challenge China's policies and practices relating to forced technology transfer and cyber-theft of U.S. trade secrets, although it did bring a WTO dispute settlement case in March 2018 against China alleged discriminatory technology licensing requirements. The European Union has brought a WTO dispute settlement case against China over certain forced technology transfer policies. See https://eeas.europa.eu/delegations/world-tradeorganization-wto/55837/eu-steps-wto-action-against-chinas-forced-technology-transfers-20-december-2018_en.

> U.S. companies are concerned that this "encouragement" will in practice amount to a "requirement" in many cases, particularly in light of the high degree of discretion provided to Chinese officials when reviewing investment applications.[7]

Ten years later, the USTR's 2012 report linked China's forced technology practices to its industrial policies and the lack of the rule of law:

> In many cases, it appears that Chinese government officials are motivated by China's industrial policy objectives when they use their unchecked power to dictate or influence foreign investment outcomes. With China's state-led economic development model, the government issues five-year plans that set objectives for virtually every sector of the economy. While these plans in broad terms seek to foster national champions, protect state-owned enterprises, promote indigenous innovation and guide the development of Chinese domestic industry up the value chain, they also include specific guidelines addressing matters such as technology transfer and the use of local content, as well as decisions about industry consolidation, production capacity, product lines and similar decisions normally made by the marketplace…Moreover, according to U.S. companies, even without formal encouragement, some Chinese government officials still consider factors such as technology transfer and the use of local content when deciding whether to approve an investment or to take some other action, such as recommend approval of a loan from a Chinese policy bank, which is often essential to the success of a project.
>
> This situation has been able to persist in part because of the absence of the rule of law in China, which fosters the use of vague and unwritten policies and does not provide for meaningful administrative or judicial review of Chinese regulatory actions, thereby enabling government officials to take unilateral actions without fear of legal challenge. Exacerbating this situation is the fact that foreign companies are hesitant to speak out publicly, or to be perceived as working with their governments to challenge China's foreign investment approval practices, because they fear retaliation from Chinese government officials.[8]

The USTR's 2018 report indicated that U.S. concerns over forced technology transfers remained:

> At the beginning of 2017, longstanding and serious U.S. concerns regarding technology transfer remained unaddressed, despite repeated, high-level bilateral commitments by China to remove or no longer pursue problematic policies and practices…Specifically, USTR found, first, that China uses foreign ownership restrictions, including joint venture requirements, equity limitations, and other investment restrictions, to require or pressure technology transfer from U.S. companies to Chinese entities. USTR also found that China uses administrative review and licensing procedures to require or pressure technology transfer, which, inter alia, undermines the value of U.S. investments and technology and weakens the global competitiveness of U.S. firms.[9]

According to the USTR, on at least eight separate occasions (from 2010to 2016) the Chinese government has committed, not to use technology transfer requirements as a condition for market access and to permit technology transfer decisions to be negotiated independently by businesses.[10] These commitments occurred through a number of bilateral fora, including the U.S.-China Joint Committee on Commerce and Trade (JCCT), the U.S.-China Strategic and Economic Dialogue (S&ED), and through statements by

[7] USTR, *2002 Report to Congress on China's WTO Compliance*, January 1, 2012, p. 27.

[8] USTR, *2012 Report to Congress on China's WTO Compliance*, December 2012, p.76.

[9] USTR, 2028 *Report to Congress on China's WTO Compliance*, February 2019, p.27.

[10] The United States has also pressed China abide by its WTO commitments on technology transfer in WTO fora, such as in the WTO's TRIP's Council. For example, in 2011, the U.S. representative to the WTO expressed concerns over China's indigenous innovation policies that sought to give preferences for government procurement contract awards to domestic Chinese firms engaged in IP and technology developing, arguing that such policies were aimed at coercing technology transfer.

Chinese leaders.[11] **Table 1** lists these commitments.[12]

Table 1. Chinese Commitments to the United States on Forced Technology Transfer

Year	Mechanism	Chinese Commitments
2010	S&ED	China reaffirmed that, consistent with WTO rules, the terms and conditions of technology transfer, production processes, and other proprietary information would be left to agreement between individual enterprises.
2011	JCCT	China confirmed that it does not and will not maintain measures that mandate the transfer of technology. China clarified that its goal obtain "mastery of core technology" for new energy vehicles (NEVs) would not require technology transfer.
2012	Then-Vice President Xi Jinping U.S. visit	China reiterated that technology transfer and technological cooperation shall be decided by businesses independently and will not be used by the Chinese government as a pre-condition for market access.
2012	S&ED	The United States and China commit to intensive, on-going discussions, including all relevant agencies, of the implementation of China's February 2012 commitment that technology transfer and technology cooperation is to be decided by businesses independently and not be used by the Chinese government as a pre-condition for market access.
2012	JCCT	China reaffirmed that technology transfer and technology cooperation are the autonomous decisions of enterprises. China will not make this a precondition for market access. If departmental or local documents contain language inconsistent with the above commitment, China will correct them in a timely manner.
2014	JCCT	Enterprises are free to base technology transfer decisions on business and market considerations, and are free to independently negotiate and decide whether and under what circumstances to assign or license intellectual property rights to affiliated or unaffiliated enterprises.
2015	President Xi's U.S. visit	China and the United States affirm the importance of developing and protecting intellectual property, including trade secrets, and commit not to advance generally applicable policies or practices that require the transfer of intellectual property rights or technology as a condition of doing business in their respective markets.
2016	President Xi's U.S. visit	The United States and China affirm the importance of developing and protecting intellectual property, including trade secrets, and commit not to advance generally applicable policies or practices that require the transfer of intellectual property rights or technology as a condition of doing business in their respective markets.

Source: CRS based on material by USTR, U.S. Department of Commerce, and U.S. Department of Treasury.

Cyber-Theft of U.S. Trade Secrets

Cyberattacks against U.S. firms have raised concerns over the potential large-scale theft of U.S. IP and its economic implications for the United States, including intrusions originating in China. To illustrate, a

[11] The JCCT was established in 1983 and is a forum for high-level dialogue on bilateral trade issues between the United States and China (seehttps://2016.export.gov/china/doingbizinchina/tradepolicydialog/eg_cn_026540.asp). The S&ED was established in 2009 by President Obama and then-Chinese President Hu Jintao to address long-term economic and strategic issues. The S&ED was a continuation of the Strategic Economic Dialogue (SED) that was initiated by President George W. Bush and President Hu Jintao in 2006. In April 2017, Presidents Trump and Xi replaced the S&ED with the U.S.-China Comprehensive Economic Dialogue (CED) to replace the S&ED (see https://www.treasury.gov/initiatives/pages/china.aspx).

[12] To the extent possible, CRS attempted to use the exact language used in official statements issued by the United States and China.

2011 report by the U.S. Office of the Director of National Intelligence (DNI) stated: "Chinese actors are the world's most active and persistent perpetrators of economic espionage. U.S. private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC (Intelligence Community) cannot confirm who was responsible." The report goes on to warn that

> China will continue to be driven by its longstanding policy of "catching up fast and surpassing" Western powers. The growing interrelationships between Chinese and U.S. companies—such as the employment of Chinese-national technical experts at U.S. facilities and the off-shoring of U.S. production and R&D to facilities in China—will offer Chinese government agencies and businesses increasing opportunities to collect sensitive US economic information.[13]

In February 2013, Mandiant, a U.S. information security company, issued a report documenting extensive economic cyberespionage by a Chinese unit (which it designated as APT1) with alleged links to the Chinese People's Liberation Army (PLA) against 141 firms, covering 20 industries, since 2006. The report stated:

> Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.[14]

In March 2013, Tom Donilon, then National Security Advisor to President Obama, called on China to recognize the urgency and scope of the cyber-security problem and the risks it poses to U.S. trade relations and the reputation to Chinese industry, take serious steps to investigate and stop cyberespionage, and to engage with the United States in a constructive dialogue to establish acceptable norms of behavior in cyberspace.[15] Following a meeting with Chinese President Xi Jinping in June 2013, President Obama warned that if Chinese cyber-theft of U.S. IP continued, then "this was going to be a very difficult problem in the economic relationship and was going to be an inhibitor to the relationship really reaching its full potential."[16] In May 2014, the U.S. Department of Justice issued a 31-count indictment against five members of the PLA for cyber-espionage and other offenses that allegedly targeted five U.S. firms and a labor union for commercial advantage, the first time the Federal government had initiated such action against state actors.[17]

In April 2015, President Obama issued Executive Order 13964 authorizing certain sanctions against "persons engaging in significant malicious cyber-enabled activates."[18] Shortly before Chinese President Xi's state visit to the United States in September 2015, some press reports indicated that the Obama Administration was considering imposing sanctions against Chinese entities over cyber theft, even possibly before the arrival of President Xi. Some analysts speculated at the time that the imposition of sanctions against China right before Xi's visit likely would have caused him to cancel his trip. This appears to have prompted China to send a high-level delegation to Washington, DC to hold four days of

[13] DNI, Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage*: 2009-2011, October 2011.

[14] Mandiant, *APT1: Exposing One of China's Cyber, Espionage Units*, February 19, 2013, p. 2.

[15] U.S. Asia Society, Complete Transcript: Thomas Donilon at Asia Society, New York March 11, 2013.

[16] National Public Radio, *Chinese Cyber-Hacking Discussed At Obama-Xi Summit*, June 9, 2013, available at http://www.npr.org/sections/thetwo-way/2013/06/09/190058558/chinese-cyber-hacking-discussed-at-obama-xi-summit.

[17] U.S. Department of Justice, at http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[18] A copy can be found at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf. The EO was extended for an additional year by President Obama on March 29, 2016.

talks in September 2015 with U.S. officials over cyber issues.[19] On September 25, 2015, Presidents Obama and Xi announced that they had reached an agreement on cyber-security and trade secrets that stated that neither country's government "will conduct or knowingly support cyber-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[20] Specifically, the sides agreed that:

- Neither country's government will conduct or knowingly support cyber-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;
- They will establish a high-level joint dialogue mechanism on fighting cybercrime and related issues;
- They will seek to work together to identify and promote appropriate norms of state behavior in cyberspace internationally; and
- Each side will provide timely responses to requests for information and assistance concerning malicious cyber activities.[21]

The two sides also agreed to set up a high-level dialogue mechanism (which would meet twice a year) to address cybercrime and improve two-way communication when cyber-related concerns arise (including the creation of a hotline). The first meeting of the *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues* was held in December 2015 in Washington, D.C. China and the United States reached agreement on a document establishing guidelines for requesting assistance on cybercrime or other malicious cyber activities and for responding to such requests. Two more meetings were held in 2016. The dialogue was continued in October 2017 under the Trump Administration.[22] The current Section 301 trade dispute between the United States and China may have led to a suspension of the dialogue.[23]

It is difficult to assess how effective the September 2015 U.S.-China cyber agreement has been in reducing the level of Chinese cyber intrusions against U.S. entities seeking to steal trade secrets as no official U.S. statistics on such activities have been make publicly available. In August 2018, Michael Moss, Deputy Director of the Cyber Threat Intelligence Integration Center stated that: "the intelligence community and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral U.S.-China cyber commitments of

[19] The White House, Press Release, September 12, 2015, available https://www.whitehouse.gov/the-press-office/2015/09/12/readout-senior-administration-officials-meeting-secretary-central.

[20] The November 2015 meeting of the G-20 countries (which includes China) included this language in its communique: "In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

[21] The White House, Fact Sheet, President Xi Jinping's State Visit to the United States, September 25, 2015, available at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[22] See U.S. Department of Justice, *Press Release*, October 6, 2017, at https://www.justice.gov/opa/pr/first-us-china-lawenforcement-and-cybersecurity-dialogue.

[23] The Diplomat, *Another US-China Dialogue Bites the Dust*, October 2, 2018, at https://thediplomat.com/2018/10/another-uschina-dialogue-bites-the-dust/.

September 2015."[24] In October 2018, CrowdStrike, a U.S. cybersecurity technology company, identified China as "the most prolific nation-state threat actor during the first half of 2018."[25] It found that Chinese entities had made targeted intrusion attempts against multiple sectors of the economy. In November 2018, FBI Director Christopher Wray stated: "No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China."[26] In December 2018, U.S. Assistant Attorney General John C. Demers stated at a Senate hearing that from 2011-2018, China was linked to more than 90% of the Justice Department's cases involving economic espionage and two-thirds of its trade secrets cases.[27]

[24] Office of the Director of National Intelligence, *Statement for the Record Mr. Michael Moss, Deputy Director Cyber Threat Intelligence Integration Center on "Cyber Threats to Our Nation's Critical Infrastructure,"* August 21, 2018, available at https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-beforethe-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center

[25] CrowdStrike, *CrowdStrike Report Reveals Cyber Intrusion Trends from Elite Team of Threat Hunters*, October 9, 2019, at https://www.crowdstrike.com/resources/news/crowdstrike-report-reveals-cyber-intrusion-trends-from-elite-team-of-threathunters/.

[26] U.S. Department of Justice, Press Release, November 1, 2018, at https://www.justice.gov/opa/pr/prc-state-owned-companytaiwan-company-and-three-individuals-charged-economic-espionage.

[27] U.S. 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, December 12, 2018, at https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf.