IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	**CASE NO. 1:18-CR-043**
Plaintiff,	:	**JUDGE TIMOTHY S. BLACK**
v.	:	**UNITED STATES' SENTENCING MEMORANDUM**
XU YANJUN a/k/a YANJUN XU,	:	
Defendant.	:	

The United States of America submits this sentencing memorandum with respect to Defendant Yanjun Xu. The government incorporates by reference the arguments made in its Memorandum Regarding Loss, filed on October 4, 2022. (R. 206, Response Memorandum Regarding the Calculation of Loss).

On November 5, 2021, a jury convicted the defendant on all counts: conspiracy to commit economic espionage (Count 1); conspiracy to commit trade secret theft (Count 2); attempted economic espionage (Count 3); and attempted trade secret theft (Count 4). For the reasons set forth below, the United States requests that the defendant be sentenced to a term of imprisonment of 300 months (25 years).

Specifically, the United States recommends a sentence of 180 months on Count 1 and 120 months on Count 2, with those sentences to run consecutive to each other. The United States recommends a sentence of 180 months on Count 3 and 120 months on Count 4, with those sentences to run consecutive to each other. The government further recommends that the sentences for Count 1 and 2 run concurrent to the sentences for Counts 3 and 4.

I. THE COURT'S TASK AT SENTENCING.

The Court must impose a sentence that is sufficient, but not greater than necessary, to achieve the purposes set forth in 18 U.S.C. § 3553(a). The factors to consider are:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed--
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> >
> > (B) to afford adequate deterrence to criminal conduct;
> >
> > (C) to protect the public from further crimes of the defendant; and
> >
> > (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
>
> (3) the kinds of sentences available;
>
> (4) the sentencing guideline range established;
>
> (5) any pertinent policy statement;
>
> (6) the need to avoid unwarranted sentence disparities; and
>
> (7) the need to provide restitution to any victims of the offense.

18 U.S.C. § 3553(a).

A Court should begin by correctly calculating the applicable Guidelines range. *Gall v. United States*, 552 U.S. 38, 49–50 (2007). The Guidelines are the starting point, but not the only consideration. The Court must consider all of the § 3553(a) factors to ascertain an appropriate sentence. *Id*. The Court may not presume that the Guidelines range is reasonable, but should make an individualized assessment based on the facts. *Id*.

II. APPLICATION OF THE SENTENCING GUIDELINES.

a. The Sentencing Guidelines Calculation.

Pursuant to the United States Sentencing Guidelines, the base offense level for the trade secret and espionage offenses is **6**. § 2B1.1(a)(2); PSR, ¶ 56.

22 levels are added due to the loss. Originally, 24 levels were added in the PSR based on an intended loss towards GE Aviation between $65 million and $150 million. PSR, ¶¶ 57-58. The defense objected to this calculation. After a hearing and additional briefing, the Court has ruled that the intended loss amount is $50.094 million, which places the loss in the range of $25 million and $65 million. U.S.S.G. § 2B1.1(b)(1)(L).

4 levels are added because the offense involves the misappropriation of a trade secret and the defendant intended to benefit a foreign government. U.S.S.G. § 2B1.1(b)(14); PSR, ¶¶ 61-62.

2 levels are added because "the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means." U.S.S.G. § 2B1.1(b)(10)(C); *United States v. Tandon,* 111 F.3d 482, 491 (6th Cir.1997) (criminal actions may constitute sophisticated means even if none of the offenses, standing alone, is "especially complex" or "especially intricate"). PSR, ¶ 60.

3 levels are added because Xu acted as a manager or supervisor of a scheme that involved five or more participants or was otherwise extensive. U.S.S.G. § 3B1.1(b); PSR, ¶¶ 64-66. The defendant objects to this enhancement.

This results in a total offense level of **37**. The defendant has a criminal history category of I. Accordingly, the guideline imprisonment range set forth in the PSR is **235 to 293 months**. The government's requested sentence – 300 months – is a slight upward variance from the range.

b. The Role in the Offense Objection.

The probation officer correctly applied a role enhancement for Xu's role in the offense. The guideline allows for 2-4 levels to be added, depending on the defendant's role in the offense. The PSR added 3 levels under this "role in the offense" provision because Xu acted as a "manager or supervisor" of the scheme that involved five or more participants or was otherwise extensive. U.S.S.G. § 3B1.1(b); PSR, ¶¶ 64-66. The defendant objects to the 3-level enhancement.

Based on the evidence presented at trial, the defendant's objection is meritless. The evidence supports either a 3 or 4-level enhancement. Here, the probation officer conservatively applied the 3-level enhancement, and her decision to apply the enhancement was correct. For example, one consideration under the provision is whether this conspiracy involved 5 or more participants. The evidence showed that, within the MSS, at least 5 people were involved in the criminal activity, including: (1) Xu Yanjun; (2) Zha Rong (Xu's supervisor) - Exs. 38, 44d, and 59b; (3) Chai Meng (a colleague in the Safran hacking, Arthur Gau, and other schemes) – Ex. 39; (4) Li Ghouzi (who worked under Xu) – Ex. 40; (5) Chen Li (a supervisor above Zha Rong) – Exs. 36 and 45; and (6) Xu Heng (who worked under Xu and came to Belgium for the GE meeting). In addition, Xu's conspiracy also pulled in people from NUAA, AVIC, COMAC, and other entities within China. The GE Aviation scheme, for example, included Xu Yanjun, Xu Heng, Zha Rong, the unnamed MSS woman that accompanied Xu to meet the GE employee, and Chen Feng (from NUAA). Exs. 50-51, 60, 64. With respect to the Safran hacking, Xu coordinated the incident through two intelligence assets whom he managed (Tian Xi and Gu

Geng), while also working with others in the MSS like Chai Meng, Zha Rong, and Song Sicheng. (Exs. 107-111). The 5-person minimum is well satisfied.

Even if the 5-person minimum were not satisfied, the "role in the offense" provision applies if the criminal activity was "otherwise extensive." As evident from the evidence at trial, the underlying offense conduct was extensive. Xu targeted multiple employees at multiple international aviation companies over multiple years. He used aliases, front companies, and false documents. He leveraged human intelligence sources, as well as cyber techniques. In addition to the extensive text-message communications presented at trial, which amounted to a multi-year written confession, Xu described the extensive scope of the MSS's work during the recorded session with Chinese engineers. The record makes plain that the criminal activity in this case was very extensive.

As to the role, a 4-level enhancement applies if the defendant is an organizer or leader. A 3-level enhancement applies if the defendant is a manager or supervisor. Although the 4-level adjustment would be justified, at a minimum, Xu should receive the 3-level enhancement as a manager or supervisor. Xu was promoted within the MSS to a Deputy Division Director with managerial responsibility over both other MSS spies and civilian intelligence assets. In that role, he coordinated sophisticated and significant intelligence operations. He directed assets and recruited co-opted employees. He supervised and directed fellow spies at the MSS in these operations, and he coordinated outreach with counterparts at AVIC and COMAC—the intended recipients of his spycraft. The 3-level adjustment is appropriate because Xu was a manager and supervisor within the conspiracy. The defense objection should be denied.

c. Applicable Upward Departures or Upward Variances.

Regardless of what loss amount the Court applies, there is a basis for upward departure under the following provisions. However, before applying an upward departure under the guidelines, the Court must first give reasonable notice to the defendant prior to sentencing. Fed. R. Crim Pro. 32(h). For a departure, the notice must specify the "ground on which the court is contemplating a departure." Or, instead of a departure under the guidelines, the Court may instead simply choose to consider these circumstances in applying the Section 3553(a) factors and find an upward variance is appropriate in this case.

U.S.S.G. § 5K2.0(a)(1)(A). The Court may depart upwards from the guideline range if there is an aggravating circumstance pursuant to 18 U.S.C. § 3553(b)(1). U.S.S.G. § 5K2.0(a)(1)(A). This requires an aggravating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines. 18 U.S.C. § 3553(b)(1). Even if the circumstance was taken into consideration, the Court can depart upward if such circumstance is present in the offense to a degree substantially in excess of that which ordinarily is involved in that kind of offense. U.S.S.G. § 5K2.0(a)(3).

The guidelines contain a modest 2-level increase in the offense level if the offense involves trade secret theft and the defendant intended to benefit a foreign government. U.S.S.G. § 2B1.1(b)(14); PSR, ¶¶ 61-62. However, this enhancement does not adequately address the conduct in this case, nor does it address the depth and breadth of the economic espionage present here. Moreover, the economic espionage effort perpetrated by Xu and the MSS over the course of his career, and against so many companies, is present to a degree that is substantially in excess of that ordinarily involved in this kind of charge. Accordingly, the Court could depart upwards

from the guidelines range because the aggravating circumstances in this case were not adequately considered in formulation of the guidelines.

U.S.S.G. § 5K2.14. The Court may also depart upwards from the guideline range pursuant to § 5K2.14 if national security, public health, or safety was significantly endangered. When this provision applies, the Court is permitted to depart upwards to reflect the nature and circumstances of the offense.

Although the term "national security" is not defined in the guidelines, the term is not limited to acts of terrorism or physical harm. The Sixth Circuit has applied a similar "national security" guideline provision to the illegal transfer of export-controlled information. *U.S. v. Hanna*, 661 F.3d 271, 290-291 and 293 (6th Cir. 2011) (shipments violating export controls are deemed to be "national security" controls). Looking at a different guideline provision that used the term "national security," the court in *Hanna* reasoned that the "national security" term can include "any offense that involves a shipment (or proposed shipment) that offends the embargo, whether or not the goods actually are intended for some innocent use." *Hanna*, 661 F.3d at 293, citing *McKeeve,* 131 F.3d 1, at 14; *see also, U.S. v. Min*, 2000 WL 1576890, (S.D. N.Y. 2000).

Using the same logic as *Hanna*, the term "national security" in § 5K2.14 can apply to economic espionage by a foreign intelligence officer like Xu.[1] As documented in the government briefs, the U.S. government has described China's efforts to illicitly acquire technology as a threat to national security.[2] Moreover, Xu openly talked about efforts to obtain

[1] Even as to the commercial engines, there are resins used that are export-controlled. (Kray, 5018-19; Davidson, 5071-72).

[2] https://www.dni.gov/files/NCSC/documents/Regulations/Foreign_Economic_Collection_2011.pdf; https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf;

U.S. military information, in addition to commercial aviation trade secrets. The body of evidence in this case weighs heavily in favor of a finding that Xu's offenses significantly endangered the national security. An upward departure is justified under § 5K2.14. In the alternative, the Court should consider these facts in its section 3553(a) analysis and vary upward.

III. THE NATURE AND CIRCUMSTANCES OF THE OFFENSE.

a. The Conspiracy to Steal Aviation Trade Secrets.

Xu's convictions in Counts 1 and 2 encompass the full scope of his operations to obtain aviation trade secrets from aviation firms (including GE) from 2013 through 2018. This includes Xu's continuous efforts to identify, assess, and recruit assets, namely ethnic Chinese insiders at Western aviation firms. Evidence at trial showed Xu's use of aliases, front companies, and universities to deceive these aviation employees and solicit information. (E.g., Exs. 43a-e). Xu even described his methods in the lengthy recording from 2017 with Chinese engineers. (Ex. 86c). Xu's efforts were not strictly limited to commercial aviation. Xu made admissions about his connection to plans for U.S. military aircraft. (Exs. 31b, 40b, 41b).

Xu and others actively selected and targeted companies that are leaders in aviation technology in the United States and around the world. Xu identified engineers and experts (co-optees) who were employed by non-Chinese aviation companies and who possessed technical expertise in the desired aviation fields. Xu and other MSS officers concealed their true identities and nature of employment with the MSS, using aliases and front organizations. Xu communicated with these co-optees regarding the types of information that the MSS wanted to

https://thehill.com/policy/national-security/528646-dni-ratcliffe-china-is-the-greatest-threat-to-democracy-and-freedom/

obtain, and the methods they should use for obtaining the desired information. On behalf of the MSS, Xu solicited, recruited, and paid such co-optees to provide technical information regarding aviation technology, including trade secret information. At times, they targeted and recruited co-optees to travel to China under the guise or false belief that the expert was traveling to China merely for "an exchange" of ideas and/or to give a presentation at a university, such as NUAA. In reality, the presentations were for the benefit of the MSS and the PRC.

Xu paid the insiders stipends and arranged for travel to China. Xu and others analyzed the stolen information with experts and determine what else was needed. This scheme was executed with full coordination between the MSS and the PRC's aviation entities. Xu laid out his work process in detail during a recorded meeting with Chinese engineers. (Exs. 86a-d).

The Safran Intrusion. The Safran-Group is a French aircraft engine manufacturer. It is also a partner with GE Aviation in a joint venture that builds engines. Xu had intelligence assets within the Safran facility in China who were willing to spy on Xu's behalf. Xu and his assets targeted a French employee of Safran that often traveled to the facility in China for work. In 2013, Xu directed one of his assets within Safran to plant malware on the French employee's Safran work computer, with the ultimate goal of being able to infiltrate the Safran network in France. The communications show Xu's integral role in the installation of the malware, his instructions to destroy the malware, and Xu's monitoring of the success and cover-up of the operation. (Ex. 110; Testimony of Adam James). Moreover, the Safran intrusion demonstrates how Xu used and could use co-opted aviation employees against their own companies. He did it with Safran, and he was attempting to do the same thing with GE Aviation.

The Hotel Room Computer Thefts. Xu's convictions also encompass his conduct in executing computer intrusions against employees of Western aviation companies that travel to China. Xu worked with others in the MSS to hack or copy the computers in hotel rooms while the aviation employees – his "guests" – were taken to dinner by the MSS. (Exs. 44a and 45a). Xu even attempted to recruit an ethnic-Chinese employee that was not an engineer, but worked exclusively in Boeing's IT department. He tried something similar with a Honeywell IT employee. (Exs. 90-93, Testimony of Sun Li).

This evidence showed that, beyond the circumstances with GE Aviation, Xu was engaged in a long-standing and determined effort to illicitly acquire technology from numerous aviation companies. To do so, he used all of the tools at his disposal, including concealing his true identity and using a sophisticated hacking scheme.

d. <u>The GE Aviation Offenses.</u>

Beginning in at least March 2017, an unindicted co-conspirator, Chen Feng, began corresponding via email with a person employed by GE as an engineer in the composite fan blade section (the "GE employee"). Chen Feng worked for an aeronautical university in Nanjing called NUAA and was an associate of Xu. Chen Feng solicited the GE employee to come to NUAA in China for an "exchange" based on the GE employee's engineering experience at GE. NUAA offered to pay for the GE employee's travel expenses. In preparation for the trip to China to present at NUAA, a message was sent to the GE employee from one of Xu's email accounts, but Xu signed the email using the name of Chen Feng. (Exs. 60b).

While the GE employee was in China, Chen Feng introduced him to Xu. Xu introduced himself using one of his aliases, Qu Hui, and claimed to be from a science and technology

association called JAST. Xu gave a business card to the GE employee that contained his alias, "Qu Hui," and contact information associated with JAST, a cover affiliation for Xu. (Ex. 63b). On June 2, 2017, the GE employee gave a presentation at NUAA in China, which included details regarding engines that were designed and produced by GE. Xu and a female MSS associate had meals with the GE employee both before and after the NUAA presentation. (Ex. 62). They paid the GE employee $3,500 in U.S. currency for the presentation and as reimbursement for expenses incurred during the visit to Nanjing.

After the trip to China, the FBI approached the GE employee and took over the communications with Chen Feng and Xu. Xu invited the GE employee to return to NUAA the following year. Chen Feng stated that he had spoken with Qu Hui (Xu) from JAST, and that Qu Hui would be able to help with travel expenses and handle the details of the "exchange." (Exs. 66, 67a-c).

The ensuing communications between Xu and the FBI (posing as the employee) fully expose Xu's efforts to recruit the GE employee as an asset and compromise GE's composite fan blade technology. On January 8, 2018, Xu wrote to the GE employee, "I will touch base with the scientific research department here to see what technology is desired and I will let you know what to prepare. For your end, please prepare the plane ticket and date as soon as possible." On January 23, 2018, Xu wrote, "Okay. Try your best to collect and we can talk by then. Domestically, there is more focused [sic] on the system code." Xu later elaborated that the information he wanted pertained to "system specification, design process," which is the application of research data to engine production. Xu provided an email address for the GE employee to use to send the requested information. (Exs. 67-74).

Xu knew that he was asking the employee to betray GE. When the GE employee informed Xu that the email may be blocked if the GE employee used the company computer, Xu responded, "It might be inappropriate to send directly from the company, right?"

On February 3, 2018, Xu caused the GE employee to send an excerpt of a presentation from GE, pertaining to "containment analysis" for a fan blade encasement. (Ex. 68). The document contained a label warning that the presentation contained proprietary information from GE. On February 4, 2018, Xu acknowledged receiving the document from GE pertaining to the "containment analysis." Xu stated that he wanted the employee to spend time talking with the experts in China for a "more precise connection." This was similar to other meetings that Xu had arranged in the past (e.g., Arthur Gau).

Xu also sent a list of technical topics pertaining to composite materials in the manufacture of fan blades and fan blade encasements that the PRC engineers were interested in, after being sent information that contained GE's proprietary warning label. Specifically, Xu wrote, the "attached file is some domestic requirements that I know of, can you take a look and let me know if you are familiar with those?" The attached list stated the following:

> *Regarding the current development situation and future development direction of foreign countries' structural materials for fan rotor blades made from composite materials:*
>
> *[A question followed.]*
>
> *Regarding the design criteria for the foreign countries' composite material rotor fan blade, stator fan blade, and fan casing:*
>
> *[A list of questions followed.]*

(Ex. 69). As explained by Jim Olson, this is an example of intelligence collection requirements that technical engineers would provide to a spy for collection. When the GE employee directly

advised Xu that some of the posed questions involved GE's commercial secrets, Xu replied they would discuss it when they met in person.

On February 5, 2018, Xu asked the GE employee to create and sort a directory of the files on the GE employee's computer relating to the files of GE. Xu asked him to send a copy of the file directory for the employee's company-issued computer. Xu sent specific directions to sort and save such a directory. When the FBI sent the computer directory, Xu's efforts to hook the employee became more aggressive. It was apparent that he thought he was on the verge of obtaining a treasure trove of highly-sensitive trade secrets from GE Aviation's composite program. (Exs. 70, 72).

Shortly after receiving the directory, Xu took the unusual step of calling the GE employee. (Ex. 75). During the call, Xu referred to the file directory and said that "they" had looked at it and it is "pretty good stuff." Xu asked if the GE employee would be able to bring it when the GE employee traveled to Europe for their meeting. Xu further stated, "the computer you will bring along is the company computer, right?" Xu also asked if the material the GE employee intended to bring could be exported out of the computer. When the GE employee informed Xu that it could be exported onto a portable hard drive, Xu replied, "Good, good, good." Xu asked, "So, if possible, we will look over the stuff. Can we do that?" After the GE employee agreed to Xu's request, Xu stated, "Do you understand? Carry the stuff along." Later in the call, Xu said: "If we need something new later, we can…talk about that in person when we meet. . . What do you think? . . All right, we really, we really don't need to rush to do everything in one time, because, if we are going to do business together, this won't be the last time, right?"

On March 4, 2018, the GE employee informed Xu that some of the documents identified on the company directory were generated from a specific software and, as a result, some documents could only be viewed and backed up when connected to GE's network. In response, Xu asked, "Does that mean I will not be able to view these documents after I bring them back?" On March 5, 2018, Xu sent the GE employee a message asking, "Regarding the document directory you sent last time, is it possible to dump it to a portable hard drive or USB drive from work computer in advance?" On March 10, 2018, Xu sent the GE employee a message stating, "Since there's still time, download more data and bring them back. Anything design related would work." These communications confirm that Xu fully intended to physically obtain the composite files during their meeting in Europe. (Exs. 76-77).

e. <u>The Conviction of Ji Chaoqun.</u>

During the trial of Xu Yanjun, the government intentionally chose not to present evidence relating to Xu's recruitment and handling of a person named Ji Chaoqun, who was separately under indictment in Chicago, Illinois and pending trial. *United States v. Ji*, Case 1:18-cr-00611, N.D. Illinois. Now that Ji Chaoqun has been convicted, the government submits the Xu Yanjun-Ji Chaoqun activity described below as conduct related to Xu's offense.[3] This information is supported by the exhibits admitted in the Ji trial, a selection of which are attached hereto. (Sentencing Memorandum, Exs. 1-10).

In September 2022, a federal jury convicted Ji Chaoqun, a Chinese national, of making a false statement and acting as an agent of the PRC without notifying the U.S. Attorney General.

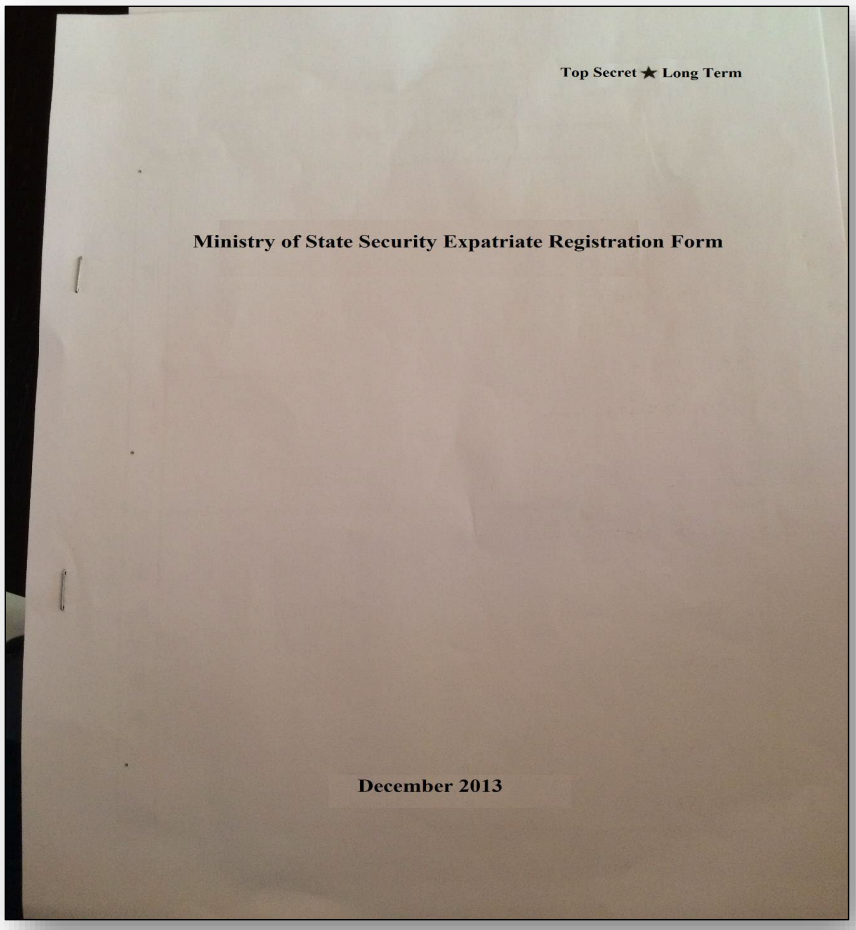
[3] Information regarding Xu's activities with Ji Chaoqun were provided to the defense through the discovery in this case. In fact, the government included this evidence in its Rule 404(b) disclosure and the defense filed a motion to exclude that evidence at trial. (R. 88 and 123).

Ji, a Chinese citizen residing in Chicago, was tasked by his MSS handler, the defendant, with providing an intelligence officer with biographical information on certain individuals for possible recruitment by the JSSD. The individuals included Chinese nationals who were working as engineers and scientists in the United States, some of whom worked for U.S. defense contractors. This tasking was part of an effort by the JSSD to obtain access to advanced aerospace and satellite technologies being developed by companies within the U.S.

As background, Ji Chaoqun was a student at the Beijing University of Aeronautics and Astronautics (BUAA) when he was recruited by Zha Rong (Xu Yanjun's boss) to join the MSS. While Ji was communicating with the MSS about potentially working on their behalf, Ji applied to study at the Illinois Institute of Technology (IIT) in Chicago. (Ex. 9). On August 22, 2013, Ji was issued his F-1 student visa to come to the United States and began his studies at IIT.

Ji traveled back to China in December 2013 and met with Xu Yanjun multiple times. (Exs. 1-2) He met with Xu on December 19, 2013, and again on January 10, 2014. At this January meeting, Xu officially registered Ji as a formal MSS overseas agent.

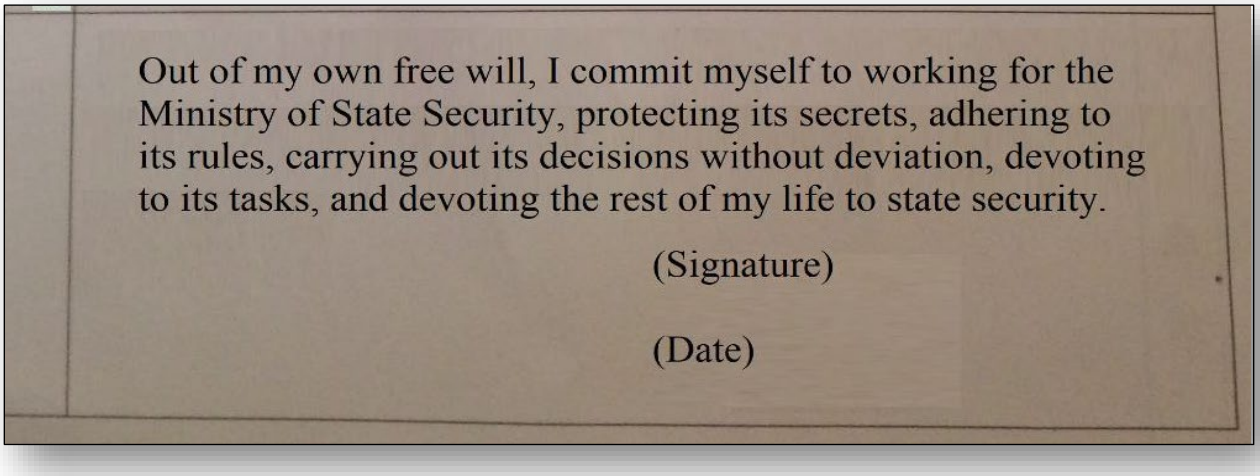
Ji took photos of the form before he signed it and the pledge it contained:



Top Secret ★ Long Term

Ministry of State Security Expatriate Registration Form

December 2013



Out of my own free will, I commit myself to working for the Ministry of State Security, protecting its secrets, adhering to its rules, carrying out its decisions without deviation, devoting to its tasks, and devoting the rest of my life to state security.

(Signature)

(Date)

(Ex. 10). At the end of the registration form was a section to describe Ji's "understanding of S&T [science and technology] intelligence work and takeaway from the training," which was consistent with the work of the Sixth Bureau to steal proprietary information related to advanced science and technology. Ji was trained by Xu and the MSS to do so in the United States.

Ji also received training on how to speak to the FBI if approached at his school. Ji took photos of this training manual. Xu gave Ji $6,000 at this January meeting, in addition to a prior payment of $5,000. Ji had successfully returned to the United States—a country with the world's most advanced aviation and military technologies—to secretly act as a spy for one of the world's premier spy agencies. He was also trained and ready.

On August 25, 2015, Xu sent Ji a screenshot of a piece of paper containing the names of eight individuals and other information about them, such as age and place of employment. (Exs. 3-8) These individuals were Chinese- and Taiwanese-American scientists who worked on advanced aviation technology, often for cleared defense contractors that built military aircraft and satellites. Just two months before Xu's tasking, China had issued the "Made in China 2025" plan that prioritized technological development of China's aerospace industry as one of ten key priority industries. After this release, Xu reached out to Ji about helping spot and assess aviation scientists in the United States—scientists who could provide technology to Chinese engineers, just as Xu explained to the AVIC engineers. *Id.*

Xu directed Ji to purchase background reports on these individuals from specific background check websites. *Id.* On August 30, 2015, Ji sent eight background check reports about these scientists by email to Xu. *Id.* As instructed by Xu, Ji compressed and encrypted the files. Ji tried to obfuscate the nature of the emails, again due to the sensitive nature of his spying

activities. *Id.* On September 18, 2015, after Xu sent Ji a ninth name to investigate, Ji sent one more background check report to Xu. As requested by Xu, Ji also gave Xu his assessments of the relative qualities of the websites. *Id.* Xu reimbursed Ji for the cost of the reports and paid him an extra approximately $500.

Ji joined the U.S. Army through a program that allowed legal aliens whose skills are considered to be vital to the national interest, such as those with language skills like Chinese fluency. On May 20, 2016, Ji enlisted in the U.S. Army Reserves through this program. Ji also told the MSS, including Xu, that he had joined the U.S. military. The only reason to give this information to an MSS officer in China was to confirm that Ji had successfully penetrated the U.S. military as an MSS agent and would be able to gather sensitive intelligence. During the Army's background check process, Ji lied and said he did not have any foreign government contacts or contacts with the MSS. Once Ji was in the Army, he could skip the many steps of the naturalization process (such as first obtaining lawful permanent residence status, *i.e.*, a green card) and go straight to citizenship. Ji did apply for citizenship.

Ji's plan was to obtain his citizenship quickly by joining the U.S. military and obtain a top-secret security clearance. He told this to an FBI undercover agent (UC) who was pretending to be an MSS agent in the United States. The UC then asked if Ji was "willing to help us [Xu and others at the MSS] to" obtain sensitive information, to which Ji responded, "Yes, I am willing." Ji offered to help other Chinese enlistees in the MAVNI program who might be willing to be recruited by the MSS. Ji reported that he had access to all military bases with his military ID and volunteered, without prompting, to take pictures of aircraft carriers for the MSS. He specified that he was able to freely enter Roosevelt-class, nuclear-powered, aircraft carriers.

The crimes committed by Ji were done on behalf of the MSS, through Xu Yanjun. Xu's handling and placement of a spy within the U.S. to obtain information regarding aviation technology and employees is yet another facet of Xu's egregious crimes towards the United States and justifies a significant sentence of imprisonment.

IV. THE HISTORY AND CHARACTERISTICS OF THE DEFENDANT.

Defendant Xu's history and characteristics were laid bare in the evidence at trial. He was a career intelligence officer. He joined the Jiangsu Ministry of State Security in 2003 and rose through the ranks over the years. (Ex. 21b). By 2009, he was the Deputy Section Chief, then quickly rose to Section Chief in 2010. In 2015, he was promoted to the Deputy Division Director in the Sixth Bureau of Jiangsu Province MSS. *Id*. Engaging in espionage was his full-time job, specializing in the acquisition of aviation technology.

The evidence at trial covered a snapshot of the last five years of his career with the MSS, from 2013 to May 2018. Evidence from that brief period shows that Xu engaged in a wide-reaching pattern of deception, computer hacking, and theft. Although Xu has no history within the United States and no criminal history, he has made a career out of committing these crimes against foreign companies, all with the assumption that he would never face consequences for his actions. Xu's history weighs in favor of a significant sentence.

The evidence at trial is illustrative of Xu's characteristics, which demonstrates that he used deceit and computer hacking to pursue his crimes. Moreover, he brought cash and pictures of the GE employee to the Belgium meeting. He was ready to engage in bribes and heavy-handed extortion of a U.S. employee to achieve his illegal objectives. These characteristics weigh heavily in favor of a significant sentence.

V. THE NEED FOR THE SENTENCE TO REFLECT THE SERIOUSNESS OF THE OFFENSE AND PROVIDE JUST PUNISHMENT.

Xu's offense can only be viewed within the context of China's broader effort to illicitly obtain trade secrets. Xu committed the crimes while acting as a trained officer and division director on behalf of the MSS, an intelligence agency for the PRC. His crimes were part of the overall PRC strategy to engage in trade-secret theft. And the seriousness of that threat to U.S. intellectual property cannot be understated.

In 2015, the PRC published "Made in China 2025," a ten-year plan that identified ten strategic technologies and industries for development. (Mulvenon, 2069). One of the identified areas was "aircraft and aircraft components (aerospace)." As stated by Hon. John Demers, "Made in China 2025" is as much roadmap to theft as it is guidance to innovate. (R. 206, Att. #2, p. 2). The PRC uses the intelligence 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." *Id*. at p. 4.

Experts have issued similar warnings. "While its goal is technological self-sufficiency, China is not taking the path of free and fair market competition to achieve this goal. Instead, China uses a variety of methods to achieve a playing field tilted entirely in its favor. . . Our companies and researchers are not competing on an equal and level playing field, but are instead up against the strategy—and power and money—of a nation-state that has the political will to see these efforts through over decades." (R. 206, Att. #3, p. 7, Testimony of Anna Puglisi).

James Mulvenon, who co-wrote the book *Chinese Industrial Espionage*, testified at trial. The net effect of the PRC's system of industrial espionage is that: (1) it allows the PRC to achieve its technological objectives with less research and development, and potentially less

money; and (2) it saves the PRC time in terms of catching up to the people who originally developed the technology. For the victim companies, if the PRC goes from being a consumer to a competitor, then it can have a negative economic impact on the company. (Mulvenon, 2088).

As stated by the U.S. Department of State, "China engages in massive intellectual-property theft. The PRC has perpetrated the greatest illegitimate transfer of wealth in human history, stealing technological innovation and trade secrets from companies, universities, and the defense sectors of the United States and other nations."[4]

In the opinion of the U.S. Director of National Intelligence, "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. It is improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of U.S. citizens—an issue we discuss in greater detail in the Online Influence Operations and Election Interference section of this report."[5]

In the opinion of James Olson, who testified at trial, the Chinese are mounting a massive espionage, cyber, and covert action assault on the United States. Their goal is to catch up to the United States technologically, militarily, and economically as quickly as possible. Olson, James

[4] Department of State, The Policy Planning Staff; The Elements of the China Challenge (December 2020), page 10.; https://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf

[5] "Worldwide Threat Assessment of the U.S. Intelligence Community"; Testimony of Dan Coats, Director of National Intelligence, Senate Select Committee on Intelligence (1/29/2019); https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1949-dni-coats-opening-statement-on-the-2019-worldwide-threat-assessment-of-the-us-intelligence-community

M., *To Catch a Spy: The Art of Counterintelligence* (2019), Georgetown University Press; p. 1. China has stolen sensitive US technology for nuclear weapons, missiles, submarines, computers, phased-array radars, military guidance systems, satellite communications, thermal imaging cameras, microwave amplifiers, night-vision goggles, and on and on. *Id*. at p. 7.

The PRC strategy is best summarized by Mr. Demers: "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." (R. 206, Att. #2, p. 5). Xu's offense conduct must be viewed within the context of the full conspiracy and the PRC's larger goal – to rob, replicate, and ultimately replace Western aviation suppliers like GE Aviation. The goal of the PRC is two-fold: (1) in serving its own population, the PRC does not want to be a customer that must purchase planes and engines from foreign companies like GE; and (2) the PRC wants to become a competitor by manufacturing its own planes and engines.

In this case, the need for the sentence to reflect the seriousness of the offense is perhaps the most significant of the 3553(a) factors, along with deterrence. The defendant must be also punished justly. "A just punishment reflects the seriousness of criminal conduct . . . [and] takes into account the consequences of a defendant's crimes, and their impact on the victims, others, and the community." *United States v. Haughawout*, 502 F. Supp. 3d 1234, 1238 (N.D. Ohio Nov. 23, 2020).

Xu's offenses were part and parcel of the MSS's plan to steal intellectual property for the benefit of the PRC. The theft relates to pieces of technology, but the ultimate goal is the theft of an entire business in order to dominate an industry. The potential consequences for the victim

companies, and for the United States as a whole, have implications for national security and economic security. These crimes in the aggregate can lead to the loss of jobs, products, and even companies. The impact can be felt at a national and local level, right down to individual families. Xu's offenses value theft over research and innovation. And Xu's offenses were not part of a single incident. Rather, his involvement was a full-time job over many years. It was part of a larger organization participating in a vast series of offenses.

Thus, the significance of these crimes cannot be overstated.

VI. PROMOTE RESPECT FOR THE RULE OF LAW AND PROTECTION OF THE PUBLIC.

The sentence must also promote respect for the rule of law generally and protect the public from further crimes of the defendant. Every day, all across this country, countless employees are entrusted with valuable, proprietary information that they need in order to do their jobs. If they disclose that information, it harms their employers. The consequences could range from mild to severe, including lost profits, lost jobs, lost opportunities, or worse.

Defendant Xu served on the front lines as a leading recruiter for that criminal activity. That was his trade. He is representative of the countries and entities that aggressively seek to plunder intellectual property from private companies. The sentence must promote respect for the rule of law among the countless employees with access to the trade secrets of American businesses, but also among the foreign governments who seek to convert such information.

In addition to those arguments of general applicability, the punishment must promote *the defendant's* respect for the rule of law. At no point in the investigation or trial did the defendant express remorse for his actions, and to the government's knowledge he has not expressed remorse at any time.

The defense disclosed an expert witness who opined, among other things, that the concept of "trade secrets" is foreign to traditional Chinese society and that, under communism, there is no private property. That is not the law in the United States – and Xu knew it. Xu understood that the insiders he targeted have an obligation to protect that information. (Ex. 67c, "It might be inappropriate to send directly from the company, right?"; Ex. 86c, "In addition, as experts abroad, it would be very difficult for them to directly take materials, large batches of materials from abroad due to the fact that their companies' security is tight. The risk they bear is very-"). But Xu targeted them anyway, because it was his singular mission to steal.

Xu had no regard for the rule of law because he never imagined that he would be standing in a U.S. courtroom to answer for his crimes. A sentence of 300 months would promote the rule of law, both widely and specifically to Xu. The sentence would also serve to protect the public from further crimes of the defendant.

VII. THE NEED TO AVOID UNWARRANTED SENTENCING DISPARITIES.

Section 3553(a)(6) of Title 18 requires that the Court consider the need to avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar conduct. This provision refers to national sentencing disparities rather than sentencing disparities among codefendants. *United States v. Simmons,* 501 F.3d 620, 623–24 (6th Cir.2007).

The Sixth Circuit has held that the Court need only accurately calculate the Guidelines range to avoid an unwarranted disparity under 18 U.S.C. § 3553(a). *See United States v. Hymes*, 19 F.4th 928, 935 (6th Cir. 2021) ("For when a district court correctly [calculates the Guidelines range], it has 'necessarily taken into account the need to avoid unwarranted sentence disparities,

viewed nationally.'" (quoting *United States v. Houston*, 529 F.3d 743, 754 (6th Cir. 2008)). Thus, in order to avoid unwarranted sentencing disparities, the Court is required only to accurately calculate and consider the Guidelines range.

However, if the Court *did* want to look to individual analogous cases, it could look at sentences following trial convictions for economic espionage. While the cases below involve domestic insiders, and Xu presents a different, and more significant threat, the Court could consider the following such sentences as a baseline:

- *United States v. Dongfan Chung*, Case No. 8:08cr24 (C.D. Cal. 2010): Dongfan Chung was convicted on seven counts of violating § 1831 (among other counts) following a bench trial. The government's recommendation as to §2B1.1 loss was $35 million (+22). Chung was sentenced to 188 months of imprisonment, including concurrent 180-month sentences for each of the 1831 counts.

- *United States v. Walter Liew*, Case No. 11cr573 (N.D. Cal. 2018): Walter Liew was convicted on two counts of violating § 1831 (among other counts) following a jury trial. §2B1.1 loss was $28 million (+22). Liew was ultimately sentenced to 144 months of imprisonment, with concurrent 120-month sentences for each of the 1831 counts.

- *United States v. Hao Zhang*, Case No. 15cr106 (N.D. Cal. 2020): Hao Zhang was convicted of multiple counts of violating §§ 1831 and 1832 following a bench trial. The government's recommendation as to §2B1.1 loss was $250,000 to $550,000 (+12). The government calculated Zhang's Guidelines range as 41–51 months of imprisonment. Zhang was sentenced to 18 months of imprisonment.

- *United States v. You*, 2022 WL 1397771, (E.D. Tenn. May 3, 2022). Defendant was convicted of attempting to steal trade secrets related to the inner coating of soda cans for the purpose of starting a competing business in China. The defendant was sentenced to 14 years imprisonment.

Finally, while not an economic espionage case, there is also Chi Mak, who worked for a defense contractor and conspired to export U.S. defense technology to China. *United States v. Chi Mak*, Case No. 8:05-cr-00293 (E.D.Cal. 2008). He was sentenced to 24 years.

When considering the potential for sentencing disparities, it's fair to say that there is no other case quite like this one. Xu's criminal conduct traces to the source of the PRC's attempts to pilfer American technology. He worked for the MSS as one of the primary recruiters who sought to identify, co-opt, and exploit insiders at U.S. companies with access to sensitive and secret technology, all for the benefit of the PRC.

VIII. ADEQUATE DETERRENCE TO CRIMINAL CONDUCT.

Section 3553(a) requires that the Court consider the need for the sentence imposed to afford adequate deterrence to criminal conduct. This factor includes two components—specific deterrence and general deterrence. Specific deterrence looks to dissuade an individual defendant from committing future crimes, while general deterrence aims to have the same effect on "the population at large." *United States v. Boucher*, 937 F.3d 702, 710 (6th Cir. 2019), citing, *United States v. Camiscione*, 591 F.3d 823, 834 (6th Cir. 2010).

Because "economic and fraud-based crimes are more rational and calculated than crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *United States v. Peppel*, 707 F.3d 627, 637 (6th Cir. 2013), quoting, *United States v. Martin,* 455 F.3d 1227, 1240 (11th Cir. 2006) (internal quotation marks, alteration, and citation omitted).

Indeed, it is critical to U.S. economic security that theft of trade secrets be discouraged in no uncertain terms. This is especially true given the difficulty of detecting the theft of trade secrets and economic espionage, crimes frequently committed by extraordinarily intelligent people entrusted with tremendous responsibility—like the defendant. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) ("Because economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes

are prime candidates for general deterrence.") (internal quotations omitted). In fact, deterrence by the prospect of punishment is critical to reducing the incidence of crimes like these. *See United States v. Courtney*, 76 F. Supp. 3d 1267, 1306 (D.N.M. Dec. 15, 2014) ("[C]rimes like this one are difficult to detect with speed or certainty, and, thus, punishment must be stepped up to effectuate general deterrence.")

These actions of Xu and the MSS towards the United States must be deterred. And, historically, there has never been an opportunity for the judicial system to provide such deterrence. The MSS conducts these economic espionage operations from within its country's borders, or through cyber-operations. It has the advantage of inviting and paying for company insiders to travel to China, where Xu and others can operate with impunity, safe from any consequences for criminal activity. It is therefore not common for the MSS officers to venture into other countries in order to meet with company insiders. (This further underscore's Xu eagerness to get a laptop from GE's composite fan module program, and the value of such information.)

This case provides a unique opportunity to send a message of deterrence to Xu and others like him who seek to steal and pillage American companies from abroad. Although this crime has become all too common, the conviction of a foreign intelligence officer who orchestrated the crimes is uncommon.

This factor should weigh heavily in the Court's determination of a just sentence. A sentence of at least 300 months is required to afford adequate deterrence to the conspiracy and pattern of espionage and theft in this case.

IX. RECOMMENDATION.

For the reasons stated above, the United States respectfully requests that Defendant Yanjun Xu be sentenced to a term of imprisonment of 300 months, or 25 years. 300 months is an appropriate sentence based on the application of the 3553(a) factors in this case, even regardless of the sentencing guideline range.

The government recommends the following breakdown of the sentence. Specifically, the United States recommends a sentence of 180 months on Count 1 and 120 months on Count 2, with those two sentences to run consecutive to each other. The United States recommends a sentence of 180 months on Count 3 and 120 months on Count 4, with those two sentences to run consecutive to each other. The government further recommends that the sentences for Count 1 and 2 run concurrent to the sentences for Counts 3 and 4.

The government recommends a term of supervised release of 3 years on each of the 4 counts.

Respectfully submitted,

KENNETH L. PARKER
United States Attorney

s/Timothy S. Mangan
TIMOTHY S. MANGAN (069287)
EMILY C. GLATFELTER
Assistant United States Attorneys
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
Office: (513) 684-3711
E-mail: Timothy.Mangan@usdoj.gov

MATTHEW MCKENZIE
Trial Attorney, U.S. Department of Justice

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Memorandum was served this 8th day of November 2022, electronically upon all counsel of record.

s/Timothy S. Mangan
TIMOTHY S. MANGAN (069287)
Assistant United States Attorney