Sentencing Economic Espionage in an Era of Great Power Competition

JENNA LIFHITS*

TABLE OF CONTENTS

* Jenna Lifhits is a fourth-year evening student at Georgetown University Law Center. The views expressed in this article are solely her own.

INTRODUCTION

Intellectual property (IP) theft costs the United States hundreds of billions of dollars a year, a figure that has only grown since the passage of the Economic Espionage Act (EEA) in 1996.[1] U.S. adversaries—especially the People's Republic of China (PRC) and Russia—are repeat perpetrators, stealing secrets to undercut America's national security. And yet, the U.S. Sentencing Commission Guidelines ("Sentencing Guidelines" or "Guidelines") used to sentence those who steal secrets for transport outside of the U.S. have not caught up with this reality. Instead, the Guidelines emphasize pecuniary loss rather than national security costs.

After 9/11, Congress oriented the Sentencing Guidelines toward the terrorism threat by creating hefty enhancements.[2] But the Guidelines have not yet been shaped to address strategic competition with the PRC, which poses the greatest overall economic and military threat to the United States.[3] The PRC's economic development strategy is premised in part on stealing U.S. research and technology.[4] However, those who steal IP to the PRC's benefit often do not receive a sentence commensurate with the national security impact of their crime.[5]

This paper will focus on prosecution of individuals who steal trade secrets in order to transport them to the PRC. While other countries also commit economic espionage, the PRC is the most significant offender.[6] This paper will begin with an overview of the PRC's economic espionage strategy, focusing on its objectives and methods to show that IP theft is a threat to U.S. national security interests.

---

1. NAT'L BUREAU OF ASIAN RSCH., COMM'N ON THE THEFT OF AM. INTELL. PROP., IP COMMISSION 2021 REVIEW: UPDATED RECOMMENDATIONS 1 (2021).

2. U.S. SENT'G GUIDELINES MANUAL § 3A1.4 (U.S. SENT'G COMM'N 2021).

3. Michael R. Gordon & Brett Forrest, *U.S. Defense Strategy Casts China as Greatest Danger to American Security*, WALL ST. J., https://www.wsj.com/articles/u-s-defense-strategy-casts-china-as-greatest-danger-to-american-security-11666885023 [https://perma.cc/AKB6-7T2X] (Oct. 27, 2022, 4:42 PM); Brooke Singeman, *China Poses 'Biggest Long-Term Threat to Economic and National Security,' FBI Director Wray Warns*, FOX NEWS (July 6, 2022, 12:25 PM), https://www.foxnews.com/politics/china-poses-biggest-long-term-threat-economic-national-security-fb-director-wray-warns [https://perma.cc/2MV4-CQ7K].

4. JOST WÜBBEKE ET AL., MADE IN CHINA 2025: THE MAKING OF A HIGH-TECH SUPERPOWER AND CONSEQUENCES FOR INDUSTRIAL COUNTRIES 7 (2016).

5. *See, e.g.*, United States v. Jin, No. 1:08-cr-00192 (N.D. Ill. Aug. 29, 2012); United States v. Pu, No. 1:11-cr-00699 (N.D. Ill. Jan. 15, 2015); United States v. Shi, No. 1:17-cr-00110 (D.D.C. Mar. 10, 2023); United States v. Tan, No. 4:19-cr-00009 (N.D. Okla Feb. 27, 2020); United States v. Zhou, No. 2:19-cr-00163 (S.D. Ohio Apr. 20, 2021); United States v. Xiang, No. 4:19-cr-00980 (E.D. Mo. Apr. 7, 2022); United States v. Yu Xue, 42 F.4th 355 (3d Cir. 2022); *see also* United States v. Jiaqiang Xu, No. 7:16-cr-00010 (S.D.N.Y. Jan. 18, 2018) (noting that "[i]t does seem as though the vast, vast majority of people sentenced under this statute are sentenced within zero to 24 months."). *But see* United States v. Yanjun Xu, No. 1:18-cr-00043 (S.D. Ohio Nov. 21, 2022); United States v. Liew, 856 F.3d 585, 595 (9th Cir. 2017).

6. *See, e.g.*, *Survey of Chinese Espionage in the United States Since 2000*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000 (last visited Jan. 12, 2024); Julian E. Barnes, *Allied Spy Chiefs Warn of Chinese Espionage Targeting Tech Firms*, N.Y. TIMES (Oct. 18, 2023), https://www.nytimes.com/2023/10/18/us/politics/china-spying-technology.html [https://perma.cc/FKN2-NJRX].

With this context in place, this paper will examine sentencing issues related to PRC-incentivized IP theft—namely, under-sentencing, uncertainty in sentencing, and a lack of focus on national security. These issues stem from several factors, but this paper will focus on the Sentencing Guidelines' emphasis on pecuniary loss. Finally, this paper will briefly touch on charging problems in foreign incentivized trade secret theft cases. Defendants in these cases—who typically receive PRC funding or other benefits—are sometimes charged with theft of trade secrets (18 U.S.C. § 1832), rather than economic espionage (18 U.S.C. § 1831), and are thereby predisposed to receive lower sentences.[7]

After surveying these issues, this paper will propose a two-fold solution: first, amend the EEA to reflect the many methods the PRC uses for technology transfer—with the aims of aligning the statute and Guidelines and putting national security concerns at the forefront of PRC-incentivized trade secret theft cases—and second, implement a corresponding sentencing structure. This new structure will eliminate the loss calculation while creating a base offense level for transporting trade secrets abroad, an enhancement for intent to benefit a foreign power, and sector-specific enhancements that recognize the PRC's military-civil fusion strategy.

I. PRC ECONOMIC ESPIONAGE STRATEGY: AN OVERVIEW

This section will discuss the PRC's objectives and methods for IP theft to contextualize both in terms of China's communist system. While IP theft often involves the theft of "civilian" technologies, the PRC's system of military-civil fusion integrates the civilian and defense sectors—meaning that seemingly innocuous civilian technologies are leveraged for defense applications. Similarly, this section will illustrate that the threat from foreign incentivized IP theft is not limited to theft of defense technologies. U.S. national security is dependent upon medical and agricultural supply chain security, for example, as much as it is defense and technology supply chains. Therefore, theft in non-defense areas is also a threat to national security.

As this section will illustrate, IP theft need not directly benefit an agency of the PRC to benefit the PRC. In the PRC's top-down system, private companies are private in name only. In reality, they are or may easily become tools of the state, such that theft benefiting a "private" PRC company is equivalent to theft benefitting the PRC government.

A. Objectives: Made in China 2025

The PRC has set its entire government apparatus and society toward "leapfrogging" the world's developed nations and dominating supply chains, standards, networks, and platforms.[8] As one retired People's Liberation Army (PLA) commander put it: "Whoever controls the flow of resources, markets, and money is

7. 18 U.S.C. §§ 1831–1832.
8. NATHAN PICARSIC & EMILY DE LA BRUYÈRE, MADE IN GERMANY, CO-OPTED BY CHINA 4 (2020).

hegemon of the world."[9] The PRC is working to meet a set of science and technology goals by 2025, 2035, and 2049—including and especially through acquiring foreign technology—to become the world leader in advanced manufacturing.

The PRC's "Made in China 2025" plan highlights ten sectors where China wants to lead: new generation information technology, aerospace equipment, high-end computerized machines and robots, marine equipment and high-end ships, advanced railway transportation equipment, new energy vehicles and energy equipment, agricultural machinery, new and advanced materials, and biopharma and high-tech medical devices.[10] China seeks to acquire and adapt foreign technology to achieve dominance in each of these areas. It has described its tech transfer process as "introduction, digestion, absorption, and re-innovation."[11]

As is clear from its Made in China 2025 priorities, the PRC is not only interested in acquiring technology with explicit military end-uses. It leverages seemingly civilian technologies for military purposes under the Chinese Communist Party's (CCP's) strategy of "Military-Civil Fusion," a whole-of-society strategy under which the PRC uses civilian technology for the ultimate end of ensuring the PLA is a "world class military" by 2049.[12] For example, the PRC could leverage purportedly civilian telecommunications networks like those provided by the PRC company Huawei for military and potential intelligence purposes, such as disrupting telecommunications networks that use Huawei equipment, or collecting personal data.[13]

Similarly, the PRC in 2020 suggested that it would use its pharmaceutical supply chain dominance against America, threatening to withhold pharmaceutical ingredients and plunge the U.S. into "the mighty sea of coronavirus."[14] Therefore, PRC theft of civilian dual-use technologies, and dominance in seemingly "civilian" areas is more than meets the eye, both because technologies in civilian sectors have military applications and because dominance in these sectors will lay the groundwork for the PRC's broader hegemony.

B. Methods: A Whole-of-Government and Whole-of-Society Strategy

The PRC has built an economic espionage infrastructure that is massive, complex, and uses "every means imaginable" to acquire foreign research and

---

9. *Id.* at 6.

10. KAREN M. SUTTER, CONG. RSCH. SERV., IF10964, "MADE IN CHINA 2025" INDUSTRIAL POLICIES: ISSUES FOR CONGRESS 1 (2023).

11. PICARSIC & BRUYÈRE, *supra* note 8, at 7.

12. U.S. DEP'T OF STATE, THE CHINESE COMMUNIST PARTY'S MILITARY CIVIL FUSION POLICY, https://2017-2021.state.gov/military-civil-fusion/[https://perma.cc/6A3L-JBS4] (last visited Nov. 4, 2023).

13. Editorial, *Huawei and the U.S.-China Tech War*, WALL ST. J. (June 9, 2020, 7:22 PM), https://www.wsj.com/articles/huawei-and-the-u-s-china-tech-war-11591744974 [https://perma.cc/5SWM-XTXS].

14. Josh Rogin, *How China is Planning to Use the Coronavirus Crisis to Its Advantage*, WASH. POST (Mar. 16, 2020, 2:14 PM), https://www.washingtonpost.com/opinions/2020/03/16/how-china-is-planning-use-coronavirus-crisis-its-advantage/ [https://perma.cc/4SBS-V2P5].

technologies.[15] It involves recruitment and collection by arms of the government, universities, seemingly private companies, professional associations, and more. The PRC has a top-down strategy that "requires the mobilization and participation of all sectors of society and the integration of civil and military resources."[16]

The PRC incentivizes IP theft through hundreds of talent recruitment programs, which exist on the national, local, and institutional levels in China.[17] The goal of these programs is to advance the PRC's science and technology goals, outlined above. Some of these programs require participants to sign legally binding contracts with PRC institutions such as universities that incentivize them to transfer intellectual capital or "set up 'shadow labs' in China working on research identical to their U.S. research."[18] Some contracts also require participants not to disclose their talent program affiliation to their U.S. employers. In exchange, participants receive funding, lab space, and more.[19] Often the PRC allows U.S.-based participants to stay in the U.S. so that the participant can maintain access to research or trade secrets and U.S. funding for their research.[20]

In addition to talent recruitment programs, the PRC strategically uses professional groups worldwide to transfer technology to China.[21] The CCP co-opts or establishes such associations to "extract and relay foreign technical information and personnel in pursuit of China's modernization."[22] Some of these groups advertise their involvement in PRC technology transfer.

Several § 1831 and § 1832 prosecutions have involved individuals who sought PRC talent program funding.[23] For example, Yu Zhou and Li Chen were sentenced for conspiracy to commit economic espionage in 2021 after they stole exosome research from Nationwide Children's Hospital in order to set up a business using the trade secrets in China.[24] Zhou was a member of the International Technology Transfer Network, and Zhou and Chen received payments from the

---

15. William C. Hannas et al., *PRC-based Technology Transfer Organizations in* CHINESE INDUSTRIAL ESPIONAGE: TECHNOLOGY ACQUISITION AND MILITARY MODERNISATION 78, 78 (2013).

16. OFF. 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 (2018).

17. STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFF., 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS 2 (Comm. Print 2019).

18. *Id.* at 2.

19. Jeffrey Stoff, *China's Talent Programs*, *in* CHINA'S QUEST FOR FOREIGN TECHNOLOGY 38, 42 (William C. Hannas & Didi Kirsten Tatlow eds., 2021).

20. FED. BUREAU OF INVESTIGATION, THE CHINA THREAT https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans [https://perma.cc/7HCY-FUFR] (last visited Nov. 4, 2023).

21. RYAN FEDASIUK & EMILY WEINSTEIN, OVERSEAS PROFESSIONALS AND TECHNOLOGY TRANSFER TO CHINA 4 (July 2020).

22. *Id.*

23. *See, e.g.*, United States v. You, No. 2:19-cr-00014 (E.D. Tenn. Feb. 22, 2022); United States v. Zheng, No. 1:19-cr-00156 (N.D.N.Y. Jan. 3, 2023).

24. Press Release, U.S. Dep't of Just., Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets, Sell Them in China (Feb. 1, 2021), https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-sell-them-china [https://perma.cc/RJT9-A6SK].

State Administration of Foreign Expert Affairs.[25] Chen also applied for grants from a PRC government entity, some of which included research and IP from Nationwide Children's Hospital.[26]

The PRC targets everyone—but especially Chinese nationals and members of the Chinese diaspora—with its tech transfer propaganda. The PRC seeks to incentivize ethnic Chinese individuals not only financially but also through propagandistic appeals to "serve the motherland."[27] The PRC looks for overseas scholars to return to China to work, return to start a company, or otherwise transfer knowledge from abroad.[28] For example, the Ministry of Education hosts an incentive program that "pays overseas Chinese scientists and engineers to 'return for short periods of time and render services to the country.'"[29] The PRC also targets non-ethnic Chinese individuals for tech transfer, especially through its academic talent recruitment programs.[30]

"Private" companies in China are a critical part of the PRC's technology acquisition strategy. The PRC, therefore, describes its efforts as "state-led, enterprise-driven."[31] In the PRC, private companies are private in name only. Any PRC-based company can be leveraged by the state for civil or military purposes. For example, under the PRC's National Intelligence Law, companies are required to "support, assist, and cooperate with state intelligence work."[32] Therefore, an individual who sets up a competitor company in the PRC based on U.S. knowhow—a common scenario in §§ 1831 and 1832 cases—is ultimately setting up a company that the PRC can use to its benefit.

II. SENTENCING FOREIGN INCENTIVIZED TRADE SECRET THEFT: THE NATIONAL SECURITY DISCONNECT

Defendants in trade secret theft cases with a foreign nexus often do not receive sentences commensurate with the national security impact of the crime committed, face uncertain sentencing outcomes, and are reminded far more often of the monetary loss they've inflicted rather than national security costs.[33] This is due to an array of factors—decisions by judges, prosecutors, defense attorneys, and the

25. Indictment as to Yu Zhou at 14, United States v. Yu Zhou, 2:19-CR-163-SDM (S.D. Ohio July 24, 2019).

26. *Id.*

27. Andrew Spear, *Serve the Motherland While Working Overseas*, *in* CHINA'S QUEST FOR FOREIGN TECHNOLOGY 21, 23 (William C. Hannas & Didi Kirsten Tatlow eds., 2021).

28. *Id.*

29. HANNAS ET AL., *supra* note 15, at 86.

30. *See, e.g.*, Press Release, U.S. Dep't of Just., Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases (Jan. 28, 2020), https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related [https://perma.cc/D97C-JKXD].

31. PICARSIC & BRUYÈRE, *supra* note 8, at 5.

32. Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017, 11:30 AM), https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense [https://perma.cc/39H6-QJBP].

33. *See, e.g.*, United States v. Hanjuan Jin, No. 1:08-cr-00192 (N.D. Ill. Aug. 29, 2012).

Sentencing Commission alike—and this paper does not purport to capture them all. Rather, this section will focus on the Guidelines' emphasis on loss. This section will then briefly touch on charging issues in cases involving foreign incentivized trade secret theft, such as where defendants are talent plan recipients.

A. Sentencing Guidelines Flaw: Loss

The Sentencing Guidelines heavily emphasize pecuniary loss in trade secret theft and economic espionage sentence calculations. The loss calculation can form the bulk of a sentence, adding up to 30 levels to a defendant's offense level, depending on the amount.[34] But as this subsection will detail, first, loss is difficult to calculate and courts vary significantly in their method for calculation—such that trade secret theft cases sometimes feature sentences that do not reflect the national security significance of the crime committed. Second, courts are disdainful of loss and have therefore varied downward in some cases, creating further uncertainty about sentencing. Third, the focus on pecuniary loss is out of touch with the EEA's emphasis on national security and sends the wrong message to defendants about the significance of their offense.

1. Difficulties Determining Loss

Loss is difficult to calculate in intellectual property theft cases even though it can be highly determinative of the length of a defendant's sentence. Under the Guidelines, loss is the "greater of actual loss or intended loss."[35] Actual loss is defined as "the reasonably foreseeable pecuniary harm that resulted from the offense," which in turn means the pecuniary harm that the defendant knew or should have known was a potential result of the offense.[36] Intended loss, meanwhile, is the pecuniary harm that the defendant "purposely sought to inflict."[37] This includes "intended pecuniary harm that would have been impossible or unlikely to occur."[38] Due to a lack of actual loss, courts often turn to intended loss—which, as of 2015, requires that a defendant have the subjective intent to purposely inflict a specific monetary amount of loss on the victim.[39] In practice, this is a high bar. Intended loss is difficult to ascertain and highly fact-specific; therefore, loss computation methods have varied significantly.

To determine intended loss, courts have used the research and development costs of the trade secret, the defendant's valuation of the trade secret or projected profits for the defendant's company, and in rare cases, gain. Each method is dependent on available evidence, and using one method of calculating loss over another can result in a significantly different sentence. This section will survey these loss calculation methods to show that the difficulty in calculating loss has,

34. U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(1) (U.S. SENT'G COMM'N 2021).
35. U.S. SENT'G GUIDELINES MANUAL § 2B1.1, app. N.(3)(A) (U.S. SENT'G COMM'N 2021).
36. *Id.* at (3)(A)(i).
37. *Id.* at (3)(A)(ii).
38. *Id.*
39. U.S. SENT'G GUIDELINES COMM'N, AMENDMENTS TO THE SENT'G GUIDELINES (Apr. 30, 2015).

at times, created a disconnect between the national security import of the theft and the length of a defendant's sentence, and has also created uncertainty for prosecutors and defendants alike.

a. Research and development costs

The government has sought to use research and development (R&D) costs in economic espionage and adjacent cases to quantify the value of a trade secret and thereby show intended loss.[40] In 2009, the Guidelines made clear that in trade secret cases, courts may consider the cost of developing the secret in estimating loss.[41] However, as described below, courts have since rejected reliance on R&D costs (and other factors, such as fair market value) to calculate intended loss without a showing that the defendant intended to inflict that particular amount of monetary loss on the victim.[42] This has made it more difficult to rely on figures that do not originate from the defendant, like R&D costs, to show loss.[43] Difficulties calculating R&D costs have, in turn, led to lower sentences.

For example, in *United States v. Yihao Pu*, in 2013 the government charged Pu with ten counts of trade secret theft, as well as wire fraud and obstruction of justice.[44] He pleaded guilty to two counts of trade secret theft.[45] Pu stole proprietary trading algorithms from financial firms that traded stocks and other assets; hard drives that Pu allegedly ordered to be "dump[ed]" outlined a plan for him to use the information he obtained to start a hedge fund in China.[46] The district court agreed with the loss calculation in the pre-sentencing report, which stated that the intended loss was $12 million, the estimated cost of development for the files Pu stole.[47] With a 20 level increase for loss, the sentencing range was 87 months to 108 months in prison.[48] However, the court sentenced Pu to 36 months in prison,

---

40. U.S. Dep't of Just., U.S. Att'ys' Bull., Prosecuting Intellectual Property Crimes, 64 § 1, 15 (2016).

41. *Id.*

42. Courts point to a 2015 revision to the Sentencing Guidelines that defines intended loss as "the pecuniary harm that the defendant *purposely sought* to inflict." U.S. SENT'G GUIDELINES COMM'N, AMEND. TO THE SENT'G GUIDELINES (Apr. 30, 2015) (emphasis added).

43. *See, e.g.*, Order Resolving Defendant's Objection to the Presentence Investigation Report's Loss Amount Computation at 10, United States v. Yanjun Xu, No. 1:18-cr-00043, 2022 U.S. Dist. LEXIS 201805 (S.D. Ohio Nov. 5, 2022). The court rejected using research and development costs because it showed PRC gain, rather than the defendant's intended loss to GE. For cases prior to the 2015 Guidelines amendment, see Tr. of Sent'g Pr. at 10, United States v. Jin, 833 F. Supp. 2d 977 (N.D. Ill. 2012); United States v. Agrawal, No. 1:10-cr-00417 (S.D.N.Y. 2010) (relying in part on the cost of developing stolen programs); United States v. Aleynikov, No. 1:10-cr-00096 (S.D.N.Y. 2010) (relying on the cost of developing the trade secret); United States v. Ameri, 412 F.3d 893, 900 (8th Cir. 2005) (drawing upon several sources, including development costs, to find loss).

44. *See* United States v. Yihao Pu, 15 F. Supp. 3d 846, 849 (N.D. Ill. 2014).

45. *See* Plea Agreement, *Yihao Pu*, 15 F. Supp. 3d 846.

46. *See* Press Release, Fed. Bureau of Investigation, Former Citadel Employee Arrested for Theft of Financial Firm's Trade Secrets (Oct. 13, 2011), https://archives.fbi.gov/archives/chicago/press-releases/2011/former-citadel-employee-arrested-for-theft-of-financial-firms-trade-secrets [https://perma.cc/JE3W-PA7W].

47. *See* United States v. Pu, 814 F.3d 818, 822 (7th Cir. 2016).

48. *Id.* at 823.

citing consideration of 18 U.S.C. § 3553(a) factors—especially the apparent lack of a greater scheme to use the stolen files.[49]

The Seventh Circuit in 2016 overruled this loss calculation as "clearly erroneous."[50] The government had not carried its burden of showing that Pu intended to cause a loss to the victim companies that totaled the cost of development of the secrets: "There is no direct evidence of how much of a loss Pu intended [the companies] to suffer."[51] To illustrate the concept of intended loss, the court gave an example of an individual who stole a credit card with a $20,000 limit but was caught before spending money using the card.[52] The appellate court reasoned that this would differ from Pu's case because there was evidence that the individual intended to make purchases until he reached the $20,000 threshold.[53]

The Seventh Circuit remanded the case based on its objection to the intended loss calculation.[54] On remand, the district court did not declare any intended or actual loss amount because counsel agreed that there was no loss.[55] The district court sentenced Pu to 18 months in prison, one-third of his original sentence—which was already a significant divergence from the Guidelines.[56]

In *United States v. Yu Xue*, the Third Circuit echoed the intended loss reasoning set forth in *Pu*.[57] Xue was an employee at GlaxoSmithKline (GSK) when she set up a pharmaceutical company in China called Renopharma, which received direct funding and support from the PRC.[58] While at GSK, Xue stole roughly 200 GSK documents, including trade secrets.[59] She pleaded guilty in 2018 to a single count of conspiracy to steal trade secrets.[60] However, the parties did not agree on loss and left that issue to the court.[61] The government claimed the loss was greater than $550 million under both the fair market value or cost of development approach, while the defense claimed the loss was $0.[62]

---

49. *Id.*

50. *Id.* at 824.

51. *Id.* at 826.

52. *Id.* at 827. However, there is almost never such a clear-cut example of ascertaining intended loss in economic espionage and trade theft cases. In addition, other circuits do not necessarily agree with the credit card limit as an example of intended loss. For example, the Third Circuit has warned that potential loss should not be automatically equated with intended loss. *See* United States v. Yu Xue, 42 F.4th 355, 364 (3d Cir. 2022).

53. United States v. Pu, 814 F.3d 818, 827 (7th Cir. 2016).

54. *Id.* at 824, 831.

55. *See* Trial of Resent'g Proceedings at 52, United States v. Yihao Pu, 15 F. Supp. 3d 846 (N.D. Ill. 2014).

56. *Id.* at 53.

57. *See Yu Xue*, 42 F.4th at 362.

58. Press Release, U.S. Dep't. of Just., Swiss Scientist Convicted by Federal Jury of Conspiracy to Steal Trade Secrets Belonging to GlaxoSmithKline (May 2, 2022), https://www.justice.gov/usao-edpa/pr/swiss-scientist-convicted-federal-jury-conspiracy-steal-trade-secrets-belonging [https://perma.cc/XW6R-ZHRX].

59. *Yu Xue*, 42 F.4th at 359.

60. *See* Gov't Mem. on Sent'g Guidelines Calculation at 2–3, United States v. Xue, No. 2:16-cr-00022 (E.D. Pa. June 15, 2016).

61. *Id.*

62. *Id.* at 14, 18.

The district court ruled that the loss amount was $0 because the government did not show that its figure—whether fair market value or development costs—reflected the loss that defendant purposefully intended GSK to suffer, "either directly or by reasonable inference."[63] As a result, Xue was sentenced to incarceration for eight months.[64] The maximum term of imprisonment under Xue's plea deal was ten years.[65] The government appealed the district court's refusal to apply an enhancement based on intended loss and lost.[66] The Third Circuit, citing *Pu*, ruled that there was a lack of evidence that Xue intended to inflict the government's asserted loss amount.[67] However, the Third Circuit disagreed with the district court's assertion that intended gain can never further an inference of intended loss.[68]

b. Projected (lost) profits

Courts have used projections of the defendant company's profits—or figures like the victim company's projected lost profits or the defendant's valuation of the market value of the stolen trade secrets—to calculate intended loss to the victim company.[69] On some occasions, courts have sought to calculate projected profits themselves, but have not been consistent in how and when they do so.[70] This creates uncertainty for sentencing.

For example, in *United States v. You*, a jury convicted Xiaorong You in 2021 for conspiracy to steal trade secrets.[71] You sought to steal trade secrets related to formulations of BPA-free can coatings in order to set up a new coating company in China.[72] She and her corporate partner received millions in PRC funding for the new company.[73] The court concluded that the market was a monopoly market, and therefore that the defendant's anticipated profits would be equivalent to

63. Op. at 37, United States v. Xue, No. 2:16-cr-00022 (E.D. Pa. Sep. 22, 2020).

64. United States v. Xue, No. 2:16-cr-00022 (E.D. Pa. June 15, 2016).

65. *See* United States v. Xue, 42 F.4th 355, 360 n.3 (3d Cir. 2022).

66. *Id.* at 365.

67. *Id.* at 363.

68. *Id.* at 365 n.9.

69. *See, e.g.*, Mem. Op. at 6–7, 9, United States v. Shan Shi, No. 1:17-cr-00110 (D.D.C. Dec. 17, 2019); Sent'g Hearing Tr. at 17, United States v. Hailong, 4:13-cr-00147 (S.D. Iowa Oct. 3, 2016); Sent'g Hearing Tr. at 39–40, United States v. Jiaqiang Xu, No. 7:16-cr-00010 (S.D.N.Y. Jan. 18, 2018). But some courts have reasoned that the defendant's belief about their potential profits shows the defendant's intended gain rather than intended loss to the victim company. *See* Op. at 37, United States v. Xue, No. 2:16-cr-00022 (E.D. Pa. Sep. 22, 2020) ("[A] trade secret theft, like the one in this case, may permit a thief to profit without an equal and opposite loss to the victim.").

70. *Compare* Mem. Op. & Order at 6, United States v. You, No. 2:19-cr-00014 (E.D. Tenn. May 3, 2022), *with* Order Resolving Def.'s Objection to Presentence Investigation Report's Loss Amount Computation at 10, United States v. Xu, No. 1:18-cr-00043 (S.D. Ohio Nov. 5, 2022).

71. Press Release, U.S. Dep't of Just., PH.D. Chemist Sentenced To 168 Months For Conspiracy To Steal Traded Secrets, Economic Espionage, Theft Of Trade Secrets, And Wire Fraud (May 9, 2022), https://www.justice.gov/usao-edtn/pr/phd-chemist-sentenced-168-months-conspiracy-steal-traded-secrets-economic-espionage [https://perma.cc/L6KW-PZ98].

72. *Id.*

73. *Id.*

intended loss.[74] The court reasoned that if the defendant were to absorb all purchases of BPA-free coatings from Chinese-owned can makers, You would bring in sales of $17.4 million a year, or $121.8 million from 2021 to 2027.[75] This resulted in a 24-level enhancement.[76] Many assumptions underlie the court's calculation, as it recognized, such as the assumption that the demand for BPA coatings in the Chinese market would neither grow nor shrink, and that the defendant would absorb all sales from Chinese-owned can manufacturers.[77] The court sentenced You to 168 months in prison, a downward variance from the Guidelines range of 324 to 405 months.[78] However, the Sixth Circuit vacated and remanded her sentence, ruling that the district court's intended loss calculation relied on market estimates that the district court itself deemed speculative, and that the court, while claiming to use anticipated profits to calculate loss, was actually using anticipated sales.[79]

In *United States v. Yanjun Xu*, the court used a similar calculation to determine loss—the competitor company's projected profits—even though the relevant market was not a monopoly.[80] A jury convicted Xu, and he was sentenced to 240 months in prison in 2022 for conspiracy to commit economic espionage, conspiracy to commit trade secret theft, and attempts of both.[81] Based on a loss computation offered by the government, the court calculated the intended loss by estimating GE Aviation's potentially lost profits due to the defendant's competing product.[82] Extending lenity to the defendant, the court assumed that a competing product from China would capture no more than one percent of GE Aviation's global business, resulting in a loss amount of $50 million, a 22-level enhancement.[83] Xu is appealing his conviction.[84]

---

74. *See* Mem. Op. & Order at 6, United States v. You, No. 2:19-cr-00014 (E.D. Tenn. May 3, 2022).

75. *Id.* at 9.

76. *Id.* at 10.

77. *Id.* at 9.

78. The government did not advocate for a sentence within the Guidelines range, asking instead for a downward variance to 240 months. Tr. of Proceedings at 64, United States v. You, No. 2:19-cr-00014 (E.D. Tenn. June 10, 2019).

79. *See* United States v. You, 74 F.4th 378, 398–99 (6th Cir. 2023).

80. Order Resolving Def.'s Objection to Presentence Investigation Report's Loss Amount Computation at 10, United States v. Yanjun Xu, No. 1:18-cr-00043 (S.D. Ohio Nov. 5, 2022); *see also* Mem. Op. at 6–7, United States v. Shi, No. 1:17-cr-00110 (D.D.C. Dec. 17, 2019) (calculating loss by examining lost profits if the competitor company had penetrated the market).

81. Press Release, U.S. Dep't of Just., Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets From Cincinnati Company (Nov. 16, 2022), https://www.justice.gov/opa/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes-attempting [https://perma.cc/CR3A-MWT2].

82. Mem. Op. & Order, *supra* note 80, at 10.

83. *Id.* at 17.

84. Yudhijit Bhattacharjee, *The Daring Ruse That Exposed China's Campaign to Steal American Secrets*, N.Y. TIMES (Mar. 7, 2023), https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html [https://perma.cc/2CPV-42JY].

c. Gain

Where courts conclude that loss cannot be determined, they sometimes turn to the defendant's gain, as per the Guidelines.[85] There is no uniform test for finding that loss cannot be determined.[86] In *United States v. Liew*, the court used the defendant's gain —in the form of payments defendant received from PRC companies—because it could not find a non-speculative way to calculate intended loss.[87] The victim company stated that loss could not be reasonably determined.[88] In 2014, the court sentenced Walter Liew to fifteen years in prison for economic espionage after a jury trial.[89]

In *United States v. Zhou*, the court used gain—in the form of evidence of payments that the defendants received related to their trade secret theft—to calculate the loss figure.[90] The parties agreed that gain was the most accurate measure of loss.[91] Yu Zhou pleaded guilty to conspiracy to steal trade secrets and wire fraud and was sentenced to 33 months in prison in 2021.[92]

2. Variances Driven by Rejections of Loss Amount

Courts are sometimes disdainful of the loss figure because they believe it results in the sentence being too low or too high, and have cited this dissatisfaction when giving downward or upward variances—creating further uncertainty in sentencing. For example, in *United States v. Xiang*, Xiang pleaded guilty in 2022 to conspiracy to commit economic espionage due to his efforts to steal proprietary algorithms from agriculture company Monsanto.[93] Xiang relied on his trade secret theft when applying for a PRC talent recruitment program, citing in his

85. U.S. SENT'G GUIDELINES MANUAL § 2B1.1, App. Note (3)(B) (U.S. SENT'G COMM'N 2021).

86. The Sixth Circuit in *Howley* stated that if a court rules that it cannot find loss, it must "engage[] in a … thorough explication of its calculation," especially where the property has "independent economic value." United States v. Howley, 707 F.3d 575, 582 (6th Cir. 2013) (citing United States v. Warshak, 631 F.3d 266, 329 (6th Cir. 2010)) (citation omitted). Another potential guardrail to using gain may be the Third Circuit's ruling that intended gain cannot be used to infer loss in trade secret cases where the record does not show that defendants used the trade secret to achieve their gain. However, that ruling was about an intended loss case, rather than a pure gain case. *See* United States v. Xue, 42 F.4th 355, 364-65 (3d Cir. 2022). In addition, the circuit court did not agree with the district court's suggestion that intended gain can never further an inference of intended loss. *Id.* at 365.

87. *See* Rep.'s Tr. of Proceedings at 12–13, United States v. Liew, No. 4:11-cr-00573-1 (N.D. Cal. July 10, 2014).

88. *See* Amend. U.S. Sent'g Mem. at 1–2, United States v. Liew, No. 4:11-cr-00573 (N.D. Cal. June 24, 2014).

89. Press Release, U.S. Dep't of Just., Walter Liew Sentenced To Fifteen Years In Prison For Economic Espionage (July 11, 2014), https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage [https://perma.cc/4X8X-BCSK].

90. *See* Tr. of Sent'g Proceedings at 4, United States v. Zhou, No. 2:19-cr-00163 (S.D. Ohio Apr. 20, 2021).

91. *Id.*

92. Press Release, U.S. Dep't of Just., Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets, Sell Them in China (Feb. 1, 2021), https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-sell-them-china [perma.cc/ZK4C-P75Y].

93. Press Release, U.S. Dep't of Just., Chinese National Sentenced for Economic Espionage Conspiracy (Apr. 7, 2022), https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-conspiracy [perma.cc/DVU5-UN26].

application the PRC's near-term goal of developing intelligent agriculture.[94] After acceptance into the program, Xiang obtained employment with the PRC and the Chinese Academy of Sciences, resigned from Monsanto, and booked a one-way ticket to the PRC.[95] The victim companies could not provide a precise loss figure.[96] The Presentence Report set forth a total offense level of 12, which equates to a range of 10 to 16 months in prison, while acknowledging that "an upward departure may be warranted" due to the absence of a loss enhancement.[97] In a rare instance of varying upward, the court concluded during sentencing that the guideline range of 0 to 16 months was "considerably lower than it should be" and sentenced Xiang to 29 months.[98]

Courts have also varied downward partly due to objections to the loss figure.[99] In *United States v. Shan Shi* in 2019, a jury found Shi guilty of conspiracy to steal trade secrets.[100] He and co-conspirators sought to steal trade secrets related to syntactic foam, a material that helps with offshore oil and gas drilling and also has military applications, for the ultimate benefit of the PRC—which has publicly emphasized its desire to develop buoyancy materials.[101] Shi applied for a talent recruitment program, stating that he would build "China's first deep-sea drilling buoyance material production line" by moving to "digest/absorb the relevant, critical U.S. technology."[102] Shi also marketed the buoyancy technology to the People's Liberation Army.[103] The court determined the loss amount to be $1 million; the applicable Guidelines range was 78 to 97 months, though the probation office recommended a downward variance to 48 months.[104] But the court sentenced Shi to 16 months in prison, pointing in part to policy objections to loss and the lack of actual loss.[105]

3. Failure to Address National Security: Guidelines versus the Economic Espionage Act

The Guidelines' focus on financial loss does not capture the national security impact of many IP theft cases. Foreign incentivized trade secret theft is a national security issue—not solely an issue of financial loss for the victim company.

---

94. *See* Gov't Sent'g Mem. at 3, 5, United States v. Xiang, No. 4:19-cr-00980 (E.D. Mo. July 23, 2021).

95. *Id.* at 1.

96. *Id.* at 10.

97. *Id.* at 15-16.

98. *See* Sent'g Hearing at 37, United States v. Xiang, No. 4:19-cr-00980 (E.D. Mo. 2021).

99. *See, e.g.*, United States v. Jin, No. 1:08-cr-00192 (N.D. Ill. Mar. 2, 2018).

100. Press Release, U.S. Dep't of Just., Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets (July 29, 2019), https://www.justice.gov/opa/pr/texas-man-convicted-conspiracy-commit-theft-trade-secrets [perma.cc/2FFU-M2JK].

101. *Id.*

102. ALEX JOSKE, HUNTING THE PHOENIX 44 (Aug. 2020).

103. *Id.*

104. Mem. Opinon at 7, United States. v. Shan Shi, 991 F.3d 198 (D.C. Cir. Feb. 10, 2020).

105. *See* Tr. of Sent'g Hearing at 73, United States v. Shan Shi, 991 F.3d 198 (D.C. Cir. Feb. 10, 2020).

However, because the loss calculation can have an outsized impact on sentencing, a significant portion of a foreign incentivized IP theft sentence can come from loss rather than a national security-related enhancement. Alternatively, because loss is difficult to calculate, plaintiffs may face sentences that do not reflect the national security impact of their offense. Both results are at odds with the EEA and send the wrong message to defendants about the significance of their offense.

The EEA intended to address a broader problem than the Sentencing Guidelines' focus on pecuniary loss. Passed in 1996, the EEA was the first federal statute to criminally prosecute foreign economic espionage.[106] By creating a cause of action to prosecute the theft of trade secrets domestically, Congress sought to protect U. S. technological leadership and national security.[107] The text of the EEA does not cabin injury to pecuniary loss. In addition, the congressional understanding of economic espionage in 1996 emphasized national security. Describing the need for the legislation in 1996, the House Judiciary Committee stated that "threats to the nation's economic interest are threats to the nation's vital security interests."[108] Congress's understanding of the connection between national security and economic espionage has only grown.[109] However, loss continues to be a significant, if not the most significant, factor in advisory Guidelines calculations in foreign economic espionage and adjacent cases.

After the base offense level of six, the most common enhancements in §§ 1831 and 1832 cases with a foreign nexus are theft to benefit a foreign government, which is a four level increase (with a minimum offense level of 14), sophisticated means, which is a two level increase, and sometimes abuse of a position of trust, which is another two level increase.[110] Meanwhile, a large loss calculation can add as many as 30 levels for crimes with more than $550 million in loss.[111] In practice, this means that cases with significant national security impact but little actual or intended loss, or a loss that is difficult to determine, receive sentences that do not reflect the severity of the offense.[112]

For example, Shan Shi—who sought to steal dual-use technology for the benefit of the PRC—was sentenced to 16 months in a downward variance due in part to policy objections to loss.[113] The loss calculation did not reflect or consider the

106. Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERK. TECH. L. J. 901, 904 (2013).

107. *Id.* at 904-05.

108. H. Rep. No. 104-788 (1996).

109. *See, e.g.*, Press Release, House Select Committee on the Chinese Communist Party, Letter to Department of Justice on Small Business Intellectual Property Theft (June 15, 2023), https://selectcommitteeontheccp.house.gov/media/letters/letter-department-justice-small-business-intellectual-property-theft [perma.cc/8AMN-D8N2].

110. U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b) (U.S. SENT'G COMM'N 2021); *id.* at § 3B1.3.

111. *Id.* at § 3B1.3.

112. *See, e.g.*, United States v. Hanjuan Jin, 833 F. Supp. 2d 977 (N.D. Ill. Aug. 29, 2012); United States v. Yihao Pu, 15 F. Supp. 3d 846 (N.D. Ill. Jan. 15, 2015); United States v. Xiang, 2021 U.S. Dist. LEXIS 199825 (E.D. Mo. 2019); United States v. Xue, 597 F. Supp. 3d 759 (E.D. Pa. Apr. 12, 2022).

113. *See* Tr. of Sent'g Hearing at 73, United States v. Shan Shi, 2020 U.S. App. LEXIS 30911 (D.C. Cir. May 28, 2020).

military value of the product Shi sought to steal. Instead, it focused on the product's market share relative to its competitors. The only apparent reflection of national security impact was a four-level enhancement for the defendant's intent to benefit a foreign government.

Because of its outsized impact on sentences and calculation disputes, loss is also a frequent focus of sentencing hearings. This muddles the message to the defendant on the significance of their crime. In reality, both the underlying statute and the effect of the crime are more about national security—of which economic security is a part—than pecuniary loss to the particular victim company. Compared to loss, courts discuss national security consequences less often, especially in § 1832 cases with a foreign nexus.[114] This matters because sentencing has an impact on the defendant's understanding of his crime, and therefore on deterrence. It is the only time the judge formally explains his rationale for his chosen sentence. Defendants should understand economic espionage or trade secret theft as the threat to national security that it is. The focus on financial loss obscures this.

B. Charging Foreign Incentivized Trade Secret Theft

In addition to issues with loss, charging decisions in cases involving foreign incentivzed trade secret theft—such as cases where the defendant receives PRC talent program funding—can predispose those cases to lower sentencing. Talent program funding is the PRC's prototypical method of incentivizing trade secret theft, as earlier discussed. Such theft, if not foreign directed, is at least foreign sponsored. A fulsome discussion of this charging issue—and its causes—is ripe for investigation.[115] This section offers only a very brief look.

Trade secret theft with a foreign nexus such as talent program funding has at times been charged under § 1832 rather than § 1831—which inclines these cases to lower sentences and diminishes their national security implications.[116] For example, in *United States v. Xue*, Yu Xue—who formed a competitor company that received direct funding and support from the PRC—was charged only with § 1832 offenses.[117] She was sentenced to incarceration for eight months. The PRC incentivizes the formation of competitor companies using stolen intellectual property. It prioritizes certain industries for intellectual property theft and

114. *See, e.g.*, Tr. of Proceeding at 69, United States v. Xiaorong You, 2021 U.S. Dist. LEXIS 47321 (E.D. Tenn. Feb. 22, 2022) ("[Loss is] what this case boils down to."); Tr. of Sent'g Hearing at 12–13, United States v. Shaoming, No. 4:13-cr-00147 (S.D. Iowa Oct. 4, 2016) ("This has been the big one since Mr. Mo pled is this issue of loss because it does drive the Guidelines so heavily.").

115. *See* Bradley Marcus & Michael Rosenberg, *Disruptive Technology Strike Force: First Prosecutions Demonstrate Difficulties in Charging Individuals with Economic Espionage*, ORRICK (June 22, 2023), https://www.orrick.com/en/Insights/2023/06/Disruptive-Technology-Strike-Force [https://perma.cc/H9V6-FD5U].

116. *See, e.g.*, Superseding Indictment, United States v. Xue, 597 F. Supp. 3d 759 (E.D. Pa. Apr. 12, 2022); U.S. Sent'g Mem. at 7, United States v. Yu Zhou, 2020 U.S. Dist. LEXIS 24319 (S.D. Ohio Apr. 20, 2021).

117. Superseding Indictment, United States v. Xue, 597 F. Supp. 3d 759 (E.D. Pa. Apr. 12, 2022).

incentivizes every facet of society to further PRC goals. Charging under § 1832 in cases like Xue's ignores this reality.

Similarly, in the case of Yu Zhou and Li Chen, the government said that the defendants' conduct "bears . . . the markers of the PRC Government's efforts to illegally transfer intellectual property from America[] to China."[118] But Zhou and Chen only faced § 1832 charges.[119] Chen applied for grant funding from a PRC government entity, and she and Chen served as experts for PRC talent plans.[120] Both Zhou and Chen received payments from the PRC's State Administration of Foreign Expert Affairs (SAFEA) for technical direction and exchange.[121]

These charging issues may be due to conflicting case law on and interpretive confusion about the EEA. In the decades since its passage, courts have diverged on interpreting § 1831 such that it is not clear that the provision captures the many methods the PRC uses to steal U.S. trade secrets.[122] This may be why prosecutors brought § 1832 charges in the earlier described cases.[123] However, § 1832 cases have a lower statutory maximum—ten years rather than fifteen for § 1831—and are less likely under the Guidelines to receive a four-level enhancement for intent to benefit a foreign government, which carries a fourteen-level minimum. In addition, § 1832 charges are not overtly associated with national security, even if the facts of the case are, unlike § 1831 charges.[124]

III. FIXING THE PROBLEM

The Sentencing Guidelines and EEA should be amended to better reflect national security concerns. First, Congress should amend the EEA by adding a section that punishes theft of a trade secret with intent to transport the secret outside of the United States. This will allow more cases to be charged using an offense that recognizes the case's foreign nexus, such as where defendants seek talent program funding or create a competing company abroad with the support of a foreign adversary. Correspondingly, the Sentencing Guidelines should be updated such that foreign economic espionage and foreign incentivized trade secret theft sentencing are placed within § 2M, the section for national defense, rather than § 2B, where economic espionage is currently.[125] This will help eliminate

118. U.S. Sent'g Mem. at 7, United States v. Yu Zhou, 2020 U.S. Dist. LEXIS 24319 (S.D. Ohio Apr. 20, 2021).

119. *Id.*

120. U.S. Sent'g Mem. at 10, United States v. Li Chen, 2021 U.S. Dist. Ct. Briefs LEXIS 3889 (S.D. Ohio Apr. 20, 2021).

121. *Id.* at 11.

122. *Compare* United States v. Lee, 2010 WL 8696087, at *1 (N.D. Cal. May 21, 2010) *with* Mem. Decision & Order at 18, United States v. Xiaoqing Zheng, 1:19-cr-00156 (N.D.N.Y. Dec. 28, 2019) (rejecting the Lee court's interpretation of § 1831). The *Lee* court's narrow judicial interpretation of § 1831 was first observed by Kuntz, *supra* note 106, at 915.

123. Examining whether § 1832 charges have in practice resulted consistently in lower sentences than § 1831 is beyond the scope of this paper, though it is a subject ripe for further research.

124. Section § 1832 was intended to cover "conventional commercial theft and misappropriation of trade secrets." *See* Lee, *supra* note 122, at *5.

125. U.S. SENT'G GUIDELINES MANUAL § 2B1.1 (U.S. SENT'G COMM'N 2021).

the problem of calculating loss. The Guidelines should also feature sector-specific enhancements that reflect national security concerns.

A. Updating the EEA

In order to better align charging with national security realities, Congress should add a provision to the EEA that punishes trade secret theft with intent to transmit the secret outside of the United States. This additional provision will help capture the variety of methods the PRC uses to steal intellectual property, including incentivizing theft for the purpose of creating a competitor company in the PRC. Such a provision will reflect the national security dimension of the offense better than § 1832. When the PRC or one of its state-owned enterprises provides a defendant with funding to create a "private" company in the PRC based on U.S. trade secrets, the law should recognize that that funding comes with strings attached and results in economic and national security benefits to the PRC.

This provision would also sync the EEA with the Sentencing Guidelines, which, based on the Foreign and Economic Espionage Penalty Enhancement Act of 2012, distinguish between the transmission of a trade secret outside of the U.S. and such transmission when it occurs with the intent to benefit a foreign government.[126] As a result of that Act, the Guidelines created an enhancement for intent to transport the secret out of the country at two levels and intent to benefit a foreign government at four levels.[127] The EEA itself does not currently reflect that structure, but it should—so that charging and sentencing are aligned.

B. Economic Espionage Under Part 2M

In order to better align sentencing with national security realities, the guideline for convictions under § 1831 and the new provision of the EEA described above should be placed under § 2M, which covers offenses involving national defense. § 2M currently houses the guidelines for espionage as well as export control violations, making it a natural home for foreign economic espionage and foreign incentivized trade secret theft.[128]

In moving these provisions under § 2M, sentencing for economic espionage and adjacent trade secret theft would no longer be based on loss—which, as earlier described, is both difficult to calculate and not aligned with the EEA itself. The § 2M Guideline could begin with a base offense level for trade secret theft with intent to transport the trade secret outside of the United States. The Guidelines would thereby reflect the PRC's top-down incentivization of trade secret theft. Individuals who seek to set up a competing corporation abroad with U.S. trade secrets—especially if they are receiving foreign government support—

126. Foreign and Economic Espionage Penalty Enhancement Act of 2012, H.R. 6029, 112th Cong (2012). A similar proposal is suggested in Kuntz, *supra* note 106.

127. U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(14) (U.S. SENT'G COMM'N 2021).

128. *Id.* at § 2M.

should receive sentences closer to those who steal secrets with clear intent to benefit a foreign government rather than those who steal secrets from a U.S. company in order to set up a rival U.S. company.

In cases with the intent to transport a trade secret outside of the U.S., the Guidelines should begin with a base offense level of around twenty. While this base offense level may appear high, defendants in foreign economic espionage and adjacent cases very often do not have a criminal record, placing their criminal history category at I. Further, an offense level in the twenties or thirties brings these cases closer to the guideline for transmitting national defense information to aid a foreign government, although it is several levels lower because not all trade secrets are equal in terms of national security impact.[129]

On top of this base offense level for intent to transmit trade secrets outside of the U.S., the Guidelines should feature an enhancement for intent to benefit a foreign government. This enhancement, which reflects 18 U.S.C. § 1831, is currently housed under § 2B.[130] It is currently a four-level enhancement associated with a minimum offense level of fourteen.[131] When moved to § 2M, this enhancement could add roughly ten levels to bring the overall offense level into the thirties, which will move economic espionage closer to the other crimes sentenced under § 2M.[132] This structure signals to courts the gravity of the crime and makes the effect of any potential downward variance, which have thus far been common, potentially less severe. It would also increase the Guidelines range for plea deals, which, as in most other cases, occur often in the economic espionage space. In general, this structure will increase sentencing ranges to reflect national security concerns and make them more consistent by removing the loss calculation.

C. Adding Sector-Specific Enhancements

The PRC has prioritized certain sectors for development in its near-term planning, signaling that these sectors have greater economic and national security value to the Chinese government. The PRC strongly incentivizes IP theft in these sectors. Therefore, theft in these areas should receive higher sentences to counter PRC incentives. This can be accomplished via a scale of sector-specific enhancements that increase in accordance with national security impact.

One measure for sector enhancements could be mapping them to the PRC's Made in China 2025 plan, which is the PRC's industrial policy that lays out the state's manufacturing goals.[133] Another potential measure is the PRC's self-identified Strategic Emerging Industries, which are eight cutting-edge areas where the government wants to boost investment: 5G, biotechnology and vaccines, high-end

129. *Id.*
130. *Id.* at § 2B1.1(b)(14).
131. *Id.*
132. *Id.* at § 2M.
133. PRC STATE COUNCIL, NOTICE OF THE STATE COUNCIL ON THE PUBLICATION OF "MADE IN CHINA 2025," *translated by* CENTER FOR SECURITY AND EMERGING TECHNOLOGY (2022).

manufacturing, new materials for airplanes and chips, new energy technologies, smart and new energy vehicles, creative digital businesses, and green technology.[134]

Sector enhancements will capture the severe national security consequences of trade secret theft in certain sectors—especially those with dual-use applications, or sectors where the U.S. is particularly vulnerable. This would incapacitate offenders who steal in these sectors for longer periods of time, helping to counteract strong incentives from the PRC to steal IP in these areas.

CONCLUSION

When a defendant steals a trade secret intending to transport it to China, the dispute is not one between a private company and a private individual. It is between a private U.S. company and an individual who has been targeted by an elaborate system, orchestrated by the PRC, of licit and illicit incentives to steal U.S. trade secrets. However, the Sentencing Guidelines do not treat economic espionage and foreign incentivized trade secret theft as such. The Guidelines treat these offenses as primarily economic when, instead, the Guidelines should treat them primarily as national security actions. The PRC's wide range of IP theft methods have outgrown the EEA's charging provisions such that defendants, whose theft is supported by the PRC and will benefit the PRC, are charged with an offense that does not reflect the national security implications of their act.

Amending the EEA to punish a broader range of foreign government-supported activity will help make judges and defendants more aware of the national security impact of adversary-supported trade secret theft. It will clarify that theft incentivized by the PRC, whether to benefit a "private" PRC company or a state-owned enterprise, is an offense much closer in nature to economic espionage than to domestic trade secret theft. A corresponding amendment to the Sentencing Guidelines that eliminates the loss calculation will increase consistency in sentencing, put the focus on national security rather than monetary loss, and provide a much-needed increase in sentencing ranges for a crime that deeply affects U.S. national security.

134. PRC NAT'L DEV. & REFORM COMM'N ET AL., GUIDING OPINIONS ON EXPANDING INVESTMENT IN STRATEGIC EMERGING NIDUSTRIES AND CULTIVATING STRENGTHENED NEW GROWTH PIONTS AND GROWTH POLES, *translated by* CENTER FOR SECURITY AND EMERGING TECHNOLOGY (2020).