IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	:	
v.	:	**Crim. No. 25-CR-322 (LLK)**
PETER WILLIAMS,	:	**Sentencing Hearing: February 24, 2026**
Defendant.	:	

UNITED STATES' MEMORANDUM IN AID OF SENTENCING

The United States of America, by and through undersigned counsel, respectfully submits this Memorandum in Aid of Sentencing. Peter Williams ("Williams" or "the Defendant") was a trusted senior corporate manager of two U.S. defense contractors that provided important cyber-tools to multiple partners of the U.S. Intelligence Community ("USIC") and other intelligence organizations in the Five Eye[1] countries. The Defendant betrayed that trust by selling eight of those same cyber-tools to a Russian zero-day[2] exploit-broker ("Russian Broker") who regularly provided exploits to Russian entities, including the Russian government. Williams sold these sensitive cyber exploits in exchange for personal profit in excess of $1.3 million. In so doing, (1) he armed the Russian Broker with advanced cyber-tools that could be re-sold to Russian and other non-NATO

[1] Five Eyes refers to a cooperation and intelligence sharing relationship between the United States, the United Kingdom, Canada, Australia and New Zealand that was formalized in a multilateral Agreement in 1946.

[2] The term zero-day exploit refers to a computer program (tool) that utilizes a vulnerability in another computer program, that is unknown to the provider of that program, to gain access to a victim's device, computer or network. Generally, once a vulnerability is discovered or known to the provider (usually through discovery by a user or security team of a compromise), the provider will then develop a computer patch to fix the vulnerability. For example, Microsoft and Apple regularly issue security patches and updates for their software. Zero-day exploits are considered the most valuable hacker tools because they are very likely to be effective against high-value targets who employ advanced cyber-defenses.

clients and used against persons around the world; (2) caused significant harm to the national security of the United States, and (3) caused serious financial and reputational damage to the defense contractors by whom he was employed, including the loss of over $35 million to Company 1 and Company 2. The United States has obtained two victim impact statements, one from Company 1 and Company 2, and a second from affected government entities which are filed as attachments to this Memorandum under seal (Exhibits 1 and 2) by separate motion to protect the trade secrets referenced therein, and to prevent further harm to the victim companies and their government customers.[3] These statements further describe the significant impact the Defendant's actions had on victims, to include specific information about the economic and reputational harm he caused.

The Defendant's conduct was sophisticated, intentional, and continued even after he was aware of an FBI investigation into the illegal activity. Given the harm caused, the egregiousness of the conduct, and other reasons discussed herein, the United States recommends that the Court sentence the Defendant to a period of incarceration at the top of the calculated guideline range under U.S. Sentencing Guidelines ("Sentencing Guidelines" or "U.S.S.G."). Specifically, based on the guidelines' calculation in the Draft Presentence Report ("PSR"),[4] this would mean a sentence of 108 months of incarceration, to be followed by three years of supervised release. The United States further seeks mandatory restitution in the amount of $35 million, as well as a forfeiture order for the items identified in the plea agreement and the consent order of forfeiture. Finally, as agreed to in the plea agreement, the parties agree the Defendant should be subject to

[3] The statements are being filed by separate motion, with a highly-sensitive document (HSD) designation pursuant to Standing Order No. 21-3 (BAH) (Jan. 12, 2021).
[4] The parties have been informed that the Final Presentence Report will not be available until February 17, 2026.

special conditions related to his access to and dissemination of proprietary and sensitive information, as well as future employment activities during the term of his incarceration and supervised release.

I. PROCEDURAL POSTURE

In or around October 2024, the FBI initiated this national security investigation into the theft of trade secrets from Company 1 and Company 2. On October 14, 2025, the United States filed an Information by consent charging the Defendant with two counts of Theft of Trade Secrets in violation of 18 U.S.C. §§1832(a)(1) and 1832(a)(2). On October 29, 2025, the Defendant pled guilty to that Information admitting to the conduct described in the Statement of Offense filed with the Court and was formally processed on those charges. After pleading guilty, the Defendant was released on conditions that included home confinement and promised to appear for his sentencing on January 27, 2026, which was continued by agreement of the parties and the Court to February 24, 2026.

II. FACTUAL SUMMARY

As described in further detail in the sworn Statement of Offense, since 2023, the Defendant has worked primarily from Company 1's offices in the District of Columbia. Company 1 sells, on behalf of Company 2, national-security focused cyber and intelligence software, including at least eight products the company sold in interstate and foreign commerce exclusively to the U.S. government and select allied governments. These eight products were treated and protected as trade secrets: Item 1, Item 2, Item 3, Item 4, Item 5, Item 6, Item 7, and Item 8 (collectively, the "Protected Products").

From at least September 2024 until August 2025, the Defendant was the General Manager of Company 1. As such, he was the primary executive in charge of Company 1's management and

its relationship with Company 2. Between 2022 and 2025, the Defendant stole software trade secrets from Company 1 and sold those trade secrets to the Russian Broker, which advertises that it acquires software and technology for various customers in Russia. The Defendant sold the Protected Products to the Russian Broker without authorization from Company 1 or Company 2 for hundreds of thousands of dollars for each Item. The Russian Broker paid the Defendant at least $1.3 million in cryptocurrency, and the Defendant then processed those proceeds through an anonymizing series of cryptocurrency transactions. The Defendant liquidated his cryptocurrency assets into cash and used the proceeds of those transactions to buy valuable items, such as luxury vacations, jewelry, watches, clothing, and properties. According to the Defendant, he spent over $715,000 in personal and family vacations between 2022 and 2025, and his purchases included the following:

Image 1- Diamond and gold jewelry listed in Preliminary Order of Forfeiture (4), (5) and (6), worth over $12,500

As part of that investigation, which began in or around October 2024, FBI special agents regularly interacted with the Defendant in late 2024 through the summer of 2025 as the primary representative of Company 1 and Company 2 who oversaw the internal corporate investigation. Over the course of several months, and multiple conversations with the FBI, the Defendant failed to acknowledge his role in the criminal activity. As the investigation progressed, the FBI agents continued to interact and interview the Defendant as the trusted corporate representative, but as they did so, they also independently uncovered evidence that implicated the Defendant in the theft and sale of these trade secrets.

In days leading up to August 6, 2025, FBI agents obtained search warrants for the Defendant's home and property and met again with the Defendant at Company 1's offices. During an initial interview on August 6, 2025, the Defendant was asked a number of questions about the criminal activity and what he knew about the Russian Broker, and he again obfuscated his own involvement. After about an hour of questioning, investigators confronted the Defendant with evidence of his guilt, including his receipt of cryptocurrency payments, contractual agreements between the Defendant's alias and the Russian Broker for the sale of cyber exploits, and the Defendant's use of that alias in anonymized email accounts. After being confronted with this evidence, the Defendant admitted his guilt and provided details of how he stole and sold trade secrets to the Russian Broker for several years through July 2025. The executed search warrants further revealed additional evidence of the Defendant's involvement in this scheme. Thereafter, the Defendant obtained counsel and continued to meet with the FBI and investigators to provide additional information about his conduct and communications with the Russian Broker. On October 9, 2025, the Defendant agreed to plead guilty and to a factual proffer.

III. SENTENCING STANDARD

In determining the sentence to be imposed, the court shall consider the factors set forth in 18 U.S.C. § 3553(a). *See* 18 U.S.C. § 3553. The court shall first consider the applicable Sentencing Guidelines range – as identified in 18 U.S.C. § 3553(a)(4)(A) – and then weigh all the factors set forth in 18 U.S.C. § 3553(a). *See, e.g.*, *Gall v. United States*, 552 U.S. 38, 49-50 (2007).

In *United States v. Booker*, 543 U.S. 220 (2005), the Supreme Court ruled that the Sentencing Guidelines are no longer mandatory. The Supreme Court subsequently explained that "the Sentencing Guidelines should be the starting point and the initial benchmark," *Gall*, 552 U.S. at 49, but they "now serve as one factor among several courts must consider in determining an appropriate sentence," *Kimbrough v. United States*, 552 U.S. 85, 92 (2007). A district court "must make an individualized assessment based on the facts presented." *Gall*, 552 U.S. at 50. If the district court determines "that an outside-Guidelines sentence is warranted, [the court] must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance." *Id.* Of note, per the terms of the plea agreement, both parties have agreed that a sentence of incarceration within the Defendant's guidelines range is the appropriate sentence and have agreed not to allocute for a variance outside that range pursuant to 18 U.S.C. §3553(a).

It is well settled that the burden to prove facts in support of a sentence is the preponderance of evidence standard. *United States v. Dorcely*, 454 F.3d 366, 371-372 (D.C. Cir. 2006); *United States v. Dozier*, 162 F.3d 120, 123 (D.C. Cir. 1998). This Court can determine a legal sentence based on all manner of information, including uncharged conduct and all of the § 3553(a) factors. *See United States v. Watts*, 519 U.S. 148, 156-157 (1997) (*per curiam*); *accord Williams v. New York*, 337 U.S. 241, 246-47 (1949); *Wasman v. United States*, 468 U.S. 559, 564 (1984) (same);

see also *Alleyne v. United States*, 570 U.S. 99 (2013) (recognizing the broad discretion of judges to select a sentence within the range authorized by law). The government here asks the Court to accept the facts in the PSR and the victim impact statements as the factual findings for sentencing purposes.

IV. ARGUMENT

This case is about how the Defendant's personal greed significantly harmed the national security of the United States and wreaked havoc on Company 1 and Company 2 and his former colleagues. The Defendant worked for over nine years in a position of trust at Company 1. He worked up the ranks at that company and U.S. Company 2 (after Company 2 acquired it), including in leadership positions, culminating in becoming the General Manager of Company 1 in September 2024. Before that, the Defendant worked in the Australian intelligence community and, by his own admission, was well-aware of how to handle sensitive material related to national security. In his time at Company 1 and Company 2, he worked as the General Manager,[5] where his income between 2022 and 2025, as shown by records from Company 1, was in excess of $2.25 million (USD). In 2024 alone his income was in excess of $775,000 from Company 1. As the General Manager of Company 1, the Defendant was trusted with knowledge of, and access to, the company's most sensitive, and proprietary technology, and he knew that the company's business involved selling intelligence software exclusively to the USIC and Five Eyes partners. At the time he chose to commit these crimes, the Defendant was a person with significant education and resources, the head of a large company, an individual with a highly paid and coveted job, with lucrative assets, living in the United States with his wife and two children. Like many who commit

[5] The position of General Manager is the highest corporate manager in Company 1, equivalent to the president of that company.

theft, however, the Defendant's desire for more money, a better lifestyle, bigger home and more jewels and trinkets- simply could not be satiated, and he chose to risk it all to betray his company, his colleagues, and the United States and its allies to satisfy that desire.

As outlined in the Statement of Offense agreed to by the Defendant, *see* Dkt. 7, the criminal conduct was sophisticated, intentional, and deceitful. Starting around April 2022 and continuing through August 2025, the Defendant used his privileged access to Company 1's protected network to avoid their corporate security protections, to locate, copy, conceal, and take away valuable trade secrets and zero-day cyber exploits off the network that he knew Company 1 had sold exclusively to USIC and other partners. He then copied and sold those trade secrets and zero-day exploits to the Russian Broker. He did so through the use of sophisticated means, encrypted communications, attempts to hide the source of cryptocurrency payments, and by lying to his supervisors and the FBI. His conduct continued even after he was aware the FBI was investigating the activity and had interviewed him about the theft of trade secrets. In his role overseeing the company's internal investigation of the thefts, he stood idly by while another employee of the company was essentially blamed for the Defendant's own conduct.

The Defendant's sale to the Russian Broker caused over $35 million in losses to Company 1 and Company 2, caused significant harm to the company's employees, and directly harmed USIC entities that used the software stolen by the Defendant and sold to the Russian Broker. As discussed in greater detail in the victim impact statements, these were not speculative harms, and the impact reverberates in the victims to this day. Additionally, by selling these powerful exploits to the Russian Broker, the Defendant made it possible for the Russian Broker to arm its clients with powerful cyber exploits that could be used against any manner of victim, civilian or military around the world, and engage in all manner of crime from cyber fraud, theft, and ransomware, to state

directed spying and offensive cyber operations against military targets. Unlike the USIC and Five Eyes countries who are limited by law and tradition in their use of cyber tools, the Russian Broker's clients were certainly not so limited. There is a reason why the Russian Broker signed contracts with the Defendant to provide him up to $4,000,000 (USD) for the Protected Products, and these contracts included additional balloon payments to maintain the efficacy of the exploits into the future.

The government acknowledges that after he was caught and confronted with evidence about his illegal activity, the Defendant confessed to the FBI agents, expressed remorse and acknowledged that he had harmed the intelligence communities of Australia and the United States. In that initial interview, he agreed to cooperate with investigators, surrender any of his property, and answer all questions from the FBI. The Defendant has done so, but his acknowledgement of responsibility (only after being confronted) and belated efforts to mitigate the harm he himself caused, do not rise to the level of "substantial assistance in the investigation or prosecution of another person who has committed an offense", as that term is used in Sentencing Guidelines, now codified as a Policy Statement at U.S.S.G. 5K1.1 (located in Appendix B of the U.S.S.G.). As such, no downward departure under the U.S.S.G. is warranted. The Defendant has already received a three-point reduction in his sentencing guidelines calculation for accepting responsibility for his actions and should not be given additional benefit, especially considering the significant harm caused in this matter. As mentioned above, the United States submits, and the parties agree per the terms of the plea agreement, that neither an upward nor downward departure or variance from the sentencing guidelines is warranted.

A. Statutory Penalties

The penalties for each count of theft of trade secrets, in violation of 18 U.S.C. § 1832(a),

include a maximum term of imprisonment of 10 years and a maximum fine of $250,000 or twice the pecuniary gain or loss of the offense, pursuant to 18 U.S.C. § 3571(b)(3). Under the Alternative Fines Act, the fine may be up to twice the pecuniary gain or "gross loss" of the offense. 18 U.S.C. § 3571(d). Since the loss applicable to Company 1 and 2 is $35 million, the maximum fine for each count allowable is $70 million. The Court can impose a period of not more than three years' supervised release but may choose not to impose such period in the case of a deportable alien, such as the Defendant. *See* 18 U.S.C. §§ 3583(b)(2); 3559(a)(3).

B. United States Sentencing Guidelines Calculation

The United States submits that, assuming the Court finds that U.S.S.G. §4C1.1 is applicable,[6] the PSR properly applies the Sentencing Guidelines to arrive at a total offense level of 29 resulting in a recommended term of incarceration of 87 to 108 months. *See* PSR at ¶ 104. Count One and Two charge the Defendant with Theft of Trade Secrets. Accordingly, U.S.S.G. § 2B1.1 applies, and the base offense level is 6. Because the loss was more than $25 million, U.S.S.G. § 2B1.1(b)(1)(L) applies and 22 levels are added, resulting in a level 28. The United States agrees with the Probation Office that the Defendant's criminal activity involved sophisticated means pursuant to U.S.S.G. §2B1.1(b)(1)(C). The United States also agrees that a two-point enhancement applies because the trade secrets were transmitted outside the United

[6] The defendant has the burden to demonstrate that the criteria of U.S.S.G. §4C1.1 ("If the defendant meets all of the following criteria") are met. *See United States v. Riley*, 376 F.3d 1160, 1170 (D.C. Cir. 2004) ("It is the defendant who bears the burden of proving by a preponderance of the evidence that he is eligible for a downward departure" (quotation omitted)). The government agrees that if the Court finds, among other things, that the Defendant did not cause "substantial financial hardship" to Company 1 or Company 2 under U.S.S.G. § 4C1.1(a)(6), then a two-level downward adjustment would be appropriate under U.S.S.G. § 4C1.1. If U.S.S.G. § 4C1.1 is inapplicable, the total offense level would be 31 with a criminal history category of I, the Sentencing Guidelines range for Williams is 107 to 135 months of imprisonment. *See* U.S.S.G. Chapter 5, Part A.

States. *See* U.S.S.G. § 2B1.1(b)(14)(A). The United States additionally agrees that a two-point enhancement applies because the Defendant abused a position of trust under U.S.S.G. § 3B1.3. The United States agrees that a three-level reduction under U.S.S.G. § 3E1.1 is applicable, as the Defendant has accepted responsibility and saved the government resources in avoiding trial.

With respect to the fine, the United States agrees with the Probation Office that, under U.S.S.G. § 5E1.2(c)(3), the fine range should be between $30,000 and $250,000. *See* U.S.S.G. § 5E1.2(c)(4).

The government acknowledges the D.C. Circuit's decision in *United States v. Smith,* 27 F.3d 649 (1994) (recognizing potential downward departure was potentially available because Jamaican defendant would not be able to spend up to six months in home confinement at the end of their sentence), that permitted a sentencing court to make a discretionary downward departure based on the Defendant's status as a removable alien. PSR at ¶¶ 130. The Defendant here is a removable alien, and he has agreed to a stipulated order of removal in this case, which means he is to be deported to Australia after his sentence is completed in the United States. However, the government believes the basis for a *Smith* departure does not exist in this matter.

The *Smith* departure is predicated on treatment of a foreign person more harshly because of their deportable status, but the opposite is true here. In *Smith*, the D.C. Circuit held that it was "permissible" to depart below a Guidelines range because of concerns that a deportable defendant might not be eligible for early release, halfway-house placement, or similar programs. 27 F.3d at 650–55. But this is discretionary, not mandatory: "a downward departure *may* be appropriate where the defendant's status as a deportable alien is likely to cause a fortuitous increase in the severity of his sentence." 27 F.3d at 655 (emphasis added). Indeed, the D.C. Circuit clarified that it "did not mean to suggest that a departure is in order whenever a factor unrelated to a prison's

just desserts may affect the severity of his confinement." *Id.* at 655. On the contrary, "the circumstances justifying a downward departure on account of the deportable alien's severity of confinement may be quite rare." *Id.*; *see also id.* ("such departures will be 'highly infrequent'" (*quoting* USSG, Ch. 1, Pt. A, § 4(b)).

The Defendant here is an Australian national who is potentially eligible to serve most of his sentence of incarceration in Australia under the terms of the International Prisoner Transfer program ("IPT"), pursuant to 18 U.S.C. §§ 4100-4115, Justice Manual §9-35, and 7 FAM §§ 480-483 (Foreign Affairs Manual). Under the terms of that program, the sentencing country (the United States), "loses jurisdiction over the prisoner's sentence, and violations of the terms or conditions of the original sentence, including supervised release, cannot be enforced even if the prisoner returns illegally to the United States after satisfying the sentence in the foreign country." Justice Manual §9-35.014 (further recognizing "it is possible for a prisoner to spend less time or more time in his home country because of differences in laws regarding applicable prison credits and the availability of different forms of conditional release").[7] Since the government understands that the Defendant will seek to avail himself of the IPT, and the Defendant's plan after incarceration is to return to Australia – where his family has already relocated – the rationale for such a *Smith* departure is not applicable, as he actually may be treated more *favorably* than other prisoners.[8]

C. Statutory Sentencing Factors of 18 U.S.C. § 3553(a)

The factors articulated in 18 U.S.C. § 3553(a) demonstrate that the imposition of a significant period of incarceration is appropriate in this case. In weighing the Section 3553(a)

[7] The government further understands that, unlike U.S. prisoners, Australian federal prisoners may obtain parole and/or early release from the Australian Attorney General. *See generally* https://www.ag.gov.au/crime/federal-offenders.

[8] The government notes that Jamaica – the home country in the *Smith* case- was never a country authorized to participated in IPT.

factors, the district court should consider: (1) the nature and circumstances of the offense; (2) and the history and characteristics of the defendant; (3) the need to promote respect for the law, to provide just punishment, to afford adequate deterrence, and to protect the public; (4) the need for educational or vocational training or medical care; and (5) the need to avoid "unwarranted sentencing disparities" among similarly situated defendants. 18 U.S.C. § 3553(a)(1), (2), (6). In addition, the sentence should reflect "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6).

1. The Nature and Circumstances of the Offenses

The nature and circumstances of the offense strongly favor a significant period of incarceration. The Defendant acted deliberately to harm his company and his colleagues, and he knew full well that his conduct would have a serious impact on the national security of the United States. The Defendant's betrayal was more than the $35 million loss to Company 1. The trade secrets stolen by the Defendant were the product of years of testing, planning, and marketing by dozens of his colleagues at Company 1, and his sale of those same crown jewels to the Russian Broker was a direct betrayal of the company and his colleagues. Specifically, Company 1 restricted its sales of powerful cyber tools and exploits to the USIC and other Five Eyes partners in order to promote the national security of the United States and its allies, and to protect them from their adversaries, like those in the Russian Federation. By allowing Company 1 to sell the Protected Products to the USIC, while he was selling the same material to the Russian Broker, the Defendant effectively denied the USIC partners the full benefit of their bargain. Instead, the Defendant maximized his own profit by playing both sides: his company, with loyalty to the USIC, and the Russian Broker whose loyalties were clearly opposed. During the period of the scheme, April 2022

to August 2025, the government estimates that the Defendant earned over $3,000,000 (USD) in total -- over $1.3 million in cryptocurrency from the Russian Broker and over $2.25 million in salary and other benefits from Company 1. The power of his greed is made plain in knowing that the Defendant was aware of a number of cyber exploit brokers in the world, including a number in the United States, but he intentionally chose to sell Company 1's trade secrets involving zero-day exploits to one of the world's most nefarious exploit brokers, the Russian Broker, simply because, by his own admission, he knew they paid the most. The Russian Broker's need to offer premium bounties is not surprising because the Russian Broker publicly advertised that its bounties for zero-day exploits were for use by non-NATO countries, and that the broker publicly stated it sold to the Russian government and Russian businesses. The exploits sold by the Defendant, which included zero-day exploits, are incredibly powerful, and would have allowed the Russian Broker and its clients to potentially access millions of computers and devices around the world, including in the United States.

Worse, of course, is that even after the breach of Company 1's trade secret became discovered by law enforcement, the Defendant continued to engage in criminal conduct and obfuscate his own involvement in the midst of an FBI and internal corporate investigation, which he oversaw. As outlined in the Statement of Offense, the Defendant became aware of the FBI investigation in the fall of 2024, but he continued to sell Company 1's trade secrets at least through July 2025—and he likely would have continued selling secrets had his scheme not been interrupted by law enforcement intervention in August 2025. Count Two of the Information specifically calls out this conduct. This combined activity permitted the Defendant to sell yet another trade secret to the Russian Broker before he was charged.

The Defendant's use of his ill-gotten proceeds is also noteworthy. He was not driven to his

crimes through some extreme financial duress, such as costs associated with life-saving medical treatment or gambling debts being collected upon penalty of death or physical harm. Instead, during the period of the conspiracy, the Defendant spent approximately $1.3 million on indulgent items such as: luxury cars (a 2022 Tesla Model X and a 2018 Porche Panamera), expensive watches, jewelry, clothing, extravagant trips and travel for himself and his family,[9] and a down payment on a house in Washington D.C. worth in excess of $1.5 million. As an example of the Defendant's extravagant purchases, he spent over $5,000 for four pieces of luxury luggage.

For more than three years – over 1,100 days – the Defendant betrayed his company and the United States. And every day of those three years, while he worked for Company 1 and 2 and outwardly affirmed his responsibilities and loyalty to the companies and their government clients, he was in truth secretly undermining their mission to protect the homeland for money from foreign adversaries. His methods were calculated and sophisticated: he used his privileged access to steal the trade secrets and exploits, he used aliases and encrypted communication to facilitate communications with the Russian Broker, and he got paid in cryptocurrency and financial transactions outside the United States to further avoid detection by law enforcement. He looked on while an internal corporate investigation falsely cast blame on his subordinate, and he worked to deceive the FBI during the investigation. And he only confessed to his crimes when he was confronted with direct evidence of them.

2. The History and Characteristics of the Offender

The Defendant is an Australian citizen who received a university degree from the University of Sydney. He has been married for over 14 years and has two children under the age

[9] As noted above, the Defendant has acknowledged that he spent over $718,000 on vacations between 2022 and 2025.

of 12, although he is not the sole caregiver. The Defendant has worked in the Australian military and was formerly employed in Australian intelligence services (which are part of the Five Eyes). He has previously had a classified security clearance in Australia, and he has been regularly trained on the proper handling of sensitive and national security information and material. He worked for nine years at Company 1 and was the highest manager in the Company before he was fired because of the instant conduct. The Defendant is presently unemployed and has no known prior criminal convictions or arrests. As outlined in the Statement of Offense and the PSR, the Defendant has significant luxury assets within the United States and Australia and has agreed to forfeit this property to the United States as part of his plea agreement and the Preliminary Order of Forfeiture. Dkt. 11. The government asks the Court to execute the Final Order of Forfeiture (which will be provided in advance of sentencing).

The Defendant has worked for Company 1 for over nine years and was intimately familiar with the nature of the tools he stole and the thousands of hours of time it took for Company 1 to create and market those tools. The government concedes that calculation of the Defendant's pay from Company 1 during the period of scheme is difficult because he received cash bonuses and reimbursements throughout the period, *see* PSR at paragraph 80 (W-2 form showing $1.7 million for 2024 and Defendant's statement that he received $31,667 a month in 2024), but the United States understands from records produced by Company 1, that he received approximately $2.25 million in income from Company 1 between 2022 and 2025. While at the company, the Defendant was regularly instructed and trained on the proper protection of those materials and the requirement to maintain those confidences even after employment with Company 1. He was also well-aware that his criminal conduct would significantly injure the company and its employees.

The Defendant's continued criminal activity with the Russian Broker after he was aware

of the FBI investigation, and as he was meeting with the FBI regularly, is evidence that he is in need of specific deterrence in the form of a period of incarceration.

The Defendant's knowledge and skill in the exploit world is well-documented, and he retains a significant amount of sensitive information that could be used by U.S. adversaries, including trade secret information and product information related to Company 1. As part of the plea agreement, the government has asked the Court to institute certain special conditions, to include conditions for supervised release, that are designed to mitigate risks that the Defendant might again betray his confidences and our country. The government requests that the Court order these conditions (both as a sentencing condition and supervised release conditions). While unlikely the defendant would try to seek to violate these conditions while in prison, the potential risk of injury in this matter, which could further harm the national security of the United States and Company 1, is also significant. We ask that this Court order these conditions during incarceration as a separate order which could be separately penalized as contempt of Court.

As an Australian citizen who is no longer on a U.S. visa, and who has signed a consent order of removal, the Defendant will be immediately subject to removal from the United States upon completion of any term of imprisonment imposed by this Court. The United States is also aware that the Defendant may seek approval to transfer his incarceration from the United States to Australia. Since pleading guilty, the Defendant has been on release and subject to home confinement. The government recognizes that after being confronted with evidence of his crimes, the Defendant has made significant efforts to try and mitigate the harm he has caused. He met with law enforcement several times and took affirmative steps to preserve his property and accounts after being advised that these accounts were subject to criminal forfeiture.[10]

[10] The government further acknowledges the Defendant may be entitled to an offset for the value

The Defendant's history and characteristics do not support a low-end Guidelines sentence, let alone a downward variance. While the defendant shares custody of two minor children, he is not their sole caretaker, and this (traditionally disfavored) factor should not weigh heavily in the Court's analysis. *See United States v. Hughes*, Nos. 04-cr-445 (CKK), 05-cv-1990 (CKK), 2006 WL 2092634, at *8 (D.D.C. July 27, 2006) (reiterating principle under previous version of the Guidelines that family ties are a "discouraged factor[]" post-*Booker*). On balance, the Defendant's intentional betrayal of his friends, his colleagues, and life's work to foreign adversaries for an even (more) luxurious life confirms that a significant period of incarceration is needed in this case.

3. The Need to Promote Respect for the Law, to Provide Just Punishment, to Afford Adequate Deterrence, and to Protect the Public

The national security implications of this case make this factor extraordinarily important. The Defendant's actions were egregious, and a significant sentence of incarceration is merited to demonstrate respect for the law, provide a just punishment, afford adequate deterrence and to protect the public for several reasons. First, stern punishment of the Defendant's conduct is vital to preserve respect for the law by federal contractors who provide sensitive material to the USIC and the military, particularly because these individuals understand the extent of the damage they cause by their illicit actions. The Defendant claimed to be protecting our national security, when in fact he was betraying it. If the Defendant were to receive a slight period of incarceration, especially after continuing the crimes while knowing the FBI was investigating the matter and interviewing him, it would send a message to other contractors that there is no downside to betraying your company and/or your country and lying to the FBI. Second, the Defendant caused

---

of the property that he has essentially pledged to provide to the victim through the government (approximately $400,000 in total) from the $35 million loss calculation pursuant to U.S.S.G. §2B1.1 Application Note 3(D)(ii). This credit, however, does not change his guideline calculation.

more than $35 million in losses to a company with employees around the world and in the District of Columbia, devastated his colleagues, and placed the country's national security at risk. As the victim impact statements show, these harms were real and the Defendant's conduct was intentional and lengthy. Third, the Defendant's conduct was highly profitable, as he signed contracts in excess of $4 million with the Russian Broker, and he received over $1.3 million in cryptocurrency payments for his sale of the Protected Products, while simultaneously collecting millions in salary and benefits from the victim companies. Fourth, the Defendant exposed our country to adversaries by selling these powerful zero-day exploits to the Russian Broker, who then re-sells those exploits to its clients. Exploit brokers such as the Russian Broker are today's modern weapon's dealers, and they are arming our adversaries with powerful weapons that can be used against almost any person around the world at the click of a mouse for any nefarious purpose, including to harm, steal, attack and/or surveil. The Defendant's (mental) retention of trade secret and other sensitive information makes this concern even greater, as a short sentence of incarceration would allow the Defendant to commit similar crimes again with information that is still fresh and (more) valuable when he would be released.

4. The Need for Educational Service, Vocational Training, or Medical Care

As described in the PSR, the Defendant does not appear to be in need of educational, vocational services or medical care at this time.

5. The Need to Avoid Unwarranted Sentencing Disparities

"The best way to curtail 'unwarranted' disparities is to follow the Guidelines, which are designed to treat similar offenses and offenders similarly." *United States v. Otunyo*, 63 F.4th 948, 960 (D.C. Cir. 2023) (*quoting United States v. Bartlett*, 567 F.3d 901, 908 (7th Cir. 2009)); *see also Gall*, 552 U.S. at 52 ("As with the seriousness of the offense conduct, avoidance of

unwarranted disparities was clearly considered by the Sentencing Commission when setting the Guidelines ranges. Since the District Judge correctly calculated and carefully reviewed the Guidelines range, he necessarily gave significant weight and consideration to the need to avoid unwarranted disparities.").

The Court should also take into account cases involving "defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). Sentences in trade secret and economic espionage cases may vary greatly based on a wide variety of circumstances, rendering exact comparison difficult. The government has found few cases involving the same combination of aggravating factors present here, including significant dollar loss associated with trade secrets, a proven harm to national security, and benefits being provided to a foreign broker who openly re-sells to foreign adversaries. Some cases that involve similar equities include:

- *United States v Dongfan Greg Chung,* 08-cr-0024 (C.D. Cal.), (violation of 18 U.S.C. § 1831): Defendant was sentenced to 188 months of incarceration after trial for trade secrets obtained from Boeing related to the Space Shuttle and Delta IV rocket for the benefit of China. *See United States v. Chung*, 633 F.Supp.2d 659 (C.D. Cal. 2009), *affirmed by* 659 F.3d 815 (9th Cir. 2011); *DOJ Press Release at* https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china .
- *United States v. Hanjin Jin*, 08-cr-00192 (N.D. Ill.) (violation of 18 U.S.C. § 1832) Defendant was convicted after trial and sentenced to 48 months of incarceration (with guideline range of 78-97 months): for stealing Motorola telecommunication trade secrets for the Chinese military. *See United States v. Hanjuan Jin*, 733 F.3d 719, 722 (7th Cir. 2013) (recognizing that "[g]iven her egregious conduct, which included

repeatedly lying to federal agents (for which she could have been prosecuted but was not), she was fortunate to be the recipient of discretionary sentencing lenity based on her ill health and inability to join her family, now in China") and *DOJ Press Release at* https://archives.fbi.gov/archives/chicago/press-releases/2012/suburban-chicago-woman-sentenced-to-four-years-in-prison-for-stealing-motorola-trade-secrets-before-boarding-plane-to-china . Notably, the Court in *Hanjin Jin*, took into consideration significant mitigating health factors that are not present in this case.

- *United States v. Yanjun Xu*, 18-cr-0043 (S.D. Ohio) (violation of 18 U.S.C. § 1831 and 1832): Defendant was convicted after trial and sentenced to 240 months of incarceration. The defendant was a Chinese intelligence officer who targeted trade secrets at numerous American aviation companies and recruited employees to travel to China to provide trade secrets to China. *See DOJ Press Release* located at https://www.justice.gov/opa/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes-attempting .
- *United States v. Kexue Huang*, 10-cr-00102 (S.D. Ind.) (violation of 18 U.S.C. § 1831) -- sentenced to 87 months of imprisonment after pleading guilty for misappropriating and selling trade secrets from Dow AgroSciences LLC and Cargill to benefit Chinese state companies who were foreign instrumentality. Unlike in this matter, loss amount calculated in the case was above $7 million, but below $20 million and guideline offense level of 27. *See DOJ Press Release* at https://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets and Docket. 91 (Government sentencing memorandum) at p. 20.
- *United States v. Chenguuang Gong*, 24-cr-00127 (C.D. Cal.) (violation of 18 U.S.C. §

1832): Defendant was sentenced to 46 months incarceration of incarceration after pleading guilty to transferring trade secret information related to technologies used by the U.S. government to detect nuclear missile launches and missiles, but no evidence indicated that the data was transferred to Chinese entities. The loss was calculated at over $3.5 million, and defendant's sentencing guideline range was 46-57 months (no adjustment for sophisticated means or abuse of trust). *See DOJ Press Release* at https://www.justice.gov/opa/pr/engineer-pleads-guilty-stealing-chinese-governments-benefit-trade-secret-technology-designed and Dkt. Entry 65 (Government Memorandum in Aid of Sentencing). Here, unlike in *Chenguuang Gong*, the Defendant in this matter did complete the transfer of protected data to the Russian Broker – not just once but on eight separate occasions, causing a loss ten times greater than the defendant in that case.

V. CONCLUSION

WHEREFORE, the United States respectfully recommends that this Court sentence the Defendant to a sentence of imprisonment for a period of 108 months. The government further requests that the Court execute the requested Consent Order of Forfeiture (which includes jewelry and other expensive property recovered from the Defendant and a $1.3 million money judgment in a forfeiture) and the requested Order of Judicial Removal proffered by the defense. The government also requests an order for $35 million in mandatory restitution, a fine of $250,000, and three years of supervised release with the special conditions of sentence and supervised release agreed to by the parties in the plea agreement and further described in PSR at paragraph 117.

Respectfully submitted,

JEANINE F. PIRRO
United States Attorney

By: ____*/s/ Tejpal Chawla*_____
Tejpal Chawla
Assistant United States Attorney
U.S. Attorney's Office, District of Columbia

JOHN A. EISENBERG
Assistant Attorney General
National Security Section

Prava Palacharla
Trial Attorney
U.S. Department of Justice
National Security Division
National Security Cyber Section

Nicholas Hunter
Trial Attorney
U.S. Department of Justice
National Security Division
Counterintelligence and Export Control Section