UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Crim. No. 25-cr-_____**
	:	
PETER WILLIAMS	:	
	:	
Defendant.	:	

STATEMENT OF OFFENSE

Pursuant to Federal Rule of Criminal Procedure 11, the United States of America, by and through its attorney, the United States Attorney for the District of Columbia, and the defendant, Peter Williams ("the defendant" or "WILLIAMS"), with the concurrence of his attorneys, John P. Rowley III and Lionel André, agree and stipulate that the below facts are true and provide a factual basis for the defendant's guilty plea. If this case were to proceed to trial, the parties stipulate that the United States could prove the below facts beyond a reasonable doubt:

The Defendant's Employment and Access to Trade Secrets

1. WILLIAMS is a citizen of Australia who has been working in the United States on a work visa since 2023. WILLIAMS has been employed by COMPANY ONE and its predecessors in Australia since at least 2016. In 2018, COMPANY ONE was fully acquired by COMPANY TWO, a publicly traded, U.S.-based company and defense contractor. Since 2023, WILLIAMS has worked primarily from COMPANY ONE's offices in the District of Columbia. COMPANY ONE sells, on behalf of COMPANY TWO, 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 and 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").

2. From at least September 2024 until August 2025, WILLIAMS was the general manager of COMPANY ONE. As such, he was the primary executive in charge of COMPANY ONE's management and its relationship with COMPANY TWO. As further described below, between 2022 and 2025, WILLIAMS stole software trade secrets from COMPANY ONE and sold those trade secrets to COMPANY THREE, a Russia-based software broker that acquires software and technology for various customers in Russia. WILLIAMS sold the trade secret software to COMPANY THREE without authorization from COMPANY ONE or COMPANY TWO for hundreds of thousands of dollars for each Item. COMPANY THREE paid WILLIAMS in cryptocurrency, and WILLIAMS then processed those proceeds through an anonymizing series of cryptocurrency transactions. WILLIAMS liquidated his cryptocurrency assets into cash and used the proceeds of those transactions to buy valuable items.

Background on COMPANY ONE and COMPANY TWO

3. COMPANY ONE is a software development company in Washington, D.C. that develops and sells cyber and intelligence software including the Protected Products. Each item contains specific components, with separate component names. COMPANY ONE has indicated that its items may be sold to its government customers as a complete product with all components included or with a subset of the components. COMPANY ONE initially developed and created these products and components and regularly updated the products and components over time. These updates are accompanied by a change in the version numbers. The updated versions of products and components are sold and distributed to customers as a part of COMPANY ONE's routine business practices. COMPANY ONE's software, including the Protected Products, is proprietary to COMPANY ONE. COMPANY ONE considers aspects of the items, including the source code and the method of structuring, implementing and designing the software, to be trade

secrets and protects those secrets with reasonable measures to preserve their confidentiality.

4. Since its purchase by COMPANY TWO, COMPANY ONE operates as a subsidiary of COMPANY TWO. According to COMPANY TWO, all products and components created by COMPANY ONE are owned and controlled by COMPANY TWO, and they are treated and protected as COMPANY TWO's trade secrets as well.

5. COMPANY ONE and COMPANY TWO protect the trade secrets in several ways. They keep the secrets confidential from third parties who do not have a need to access the secrets. The companies also do not publish their secrets, unlike patents. COMPANY ONE sells the Protected Products only to trusted government customers who have contractual obligations limiting the use and redistribution of the products. Additionally, COMPANY ONE's products are developed and stored on its internal, access-controlled, multi-factor authenticated, secure network (the "Secure Network"). When employees work outside the Secure Network, they are required to use "air-gapped"[1] computers whose ability to access communications networks has been disabled. According to COMPANY TWO, not all employees have access to COMPANY ONE's products on the Secure Network. Instead, it is restricted to those who have a need to know within the business and this access such accesses are monitored and controlled.

6. COMPANY ONE and COMPANY TWO also use physical security measures to secure their facilities against entry by unauthorized persons. These physical security measures include digital card-swipe door access, personal identification number codes, personal safes offered to U.S. employees to lock company equipment, and radio-frequency (RF) shielded boxes.

7. According to COMPANY TWO, COMPANY ONE's sales of the Protected

[1] An "air gap" refers to a security measure where a computer network or device is physically or logically isolated from other networks, particularly those connected to the internet, to prevent unauthorized access and cyberattacks. This isolation can be achieved through physical disconnection, logical separation, or a combination of both. Air gaps are primarily used to protect sensitive or critical systems from external threats by limiting the potential attack surface.

Products are closely monitored by COMPANY TWO. New employees must agree to maintain the confidentiality of all of COMPANY TWO's proprietary and confidential information, which includes all products and components developed by COMPANY ONE. All employees for COMPANY ONE and COMPANY TWO must also complete a proprietary information training course, which was launched in 2019, within sixty days of hiring and involves periodic updates and recertifications.

8. WILLIAMS has completed multiple trainings required by COMPANY TWO, including trainings on Code of Conduct, Insider Threat, Security Awareness, Global Trade Compliance, Australia Export Control, Anti-Corruption Compliance, Cybersecurity, Trade Compliance General Awareness, and Trade Compliance Stakeholder Training for Locations Outside of the U.S. These trainings relate to protecting all of COMPANY TWO's proprietary information and government-customer information, including the information owned by COMPANY ONE. These trainings discuss COMPANY TWO's proprietary information, which includes trade secrets. During a voluntary interview with the FBI on July 2, 2025, WILLIAMS affirmed that he considered all COMPANY ONE items to be trade secrets.

9. Given his tenure in COMPANY ONE, WILLIAMS maintained "super-user" access to the Secure Network. As a super-user, WILLIAMS could view all activity, logs, and data associated with the Secure Network, including the Protected Products. WILLIAMS's company network access gave him full access to COMPANY ONE's proprietary information and trade secrets.

Discovery of Theft of Trade Secrets and Internal Investigation

10. In or about October 2024, COMPANY ONE was alerted that COMPANY ONE's products had leaked and were possessed by an unauthorized software broker. COMPANY ONE initiated an internal review in which WILLIAMS oversaw a trusted COMPANY ONE

investigator. Despite being a fiduciary to COMPANY ONE and COMPANY TWO, WILLIAMS did not disclose to the investigator, COMPANY ONE, COMPANY TWO, or any trusted government customers that he had stolen the Protected Products and illegally sold them to COMPANY THREE. As part of the internal inquiry, COMPANY ONE confirmed that an unauthorized vendor outside of the United States was selling a component of Item 3 by comparing company-specific vendor data found on a stolen component that matched COMPANY ONE files on Item 3.

11. WILLIAMS was regularly updated about the COMPANY ONE internal inquiry and its ultimate conclusion that COMPANY ONE was unaware of any unauthorized intrusion into the company's network outside of a former employee who, while employed, had improperly accessed the internet from an air-gapped device. At no time did WILLIAMS disclose to COMPANY ONE or COMPANY TWO that he stole the trade secrets or that he sold those secrets to COMPANY THREE. COMPANY ONE and COMPANY TWO provided the results of the internal inquiry to the Federal Bureau of Investigation ("FBI") in or about November 2024.

12. The FBI investigation of the reported activity involved interviewing representatives from COMPANY ONE, including WILLIAMS. During a voluntary interview with the FBI on July 2, 2025, WILLIAMS described COMPANY ONE's training as having been intended to keep COMPANY ONE's products from "hitting the internet." WILLIAMS further described semi-annual training mandated by COMPANY TWO, which included insider-threat training, cybersecurity training and additional training required by COMPANY ONE. WILLIAMS also indicated the most likely way for a product to be released from the Secure Network without internal indications of compromise is for an individual with access to the Secure Network to download the source material for a product from the Secure Network and transfer it to an air-gapped device (*i.e.*, a device not connected to an electronic network), like a mobile telephone or

external drive. In that same interview, WILLAMS estimated the loss to COMPANY ONE for the compromise of Items 1 and 3 to be approximately $35 million.

WILLIAMS's Sale of Stolen Protected Products to COMPANY THREE

13. COMPANY THREE is based in Russia and advertises itself as a Russian zero-day purchase platform. COMPANY THREE advertises that its clients are Russian private and government organizations.

14. COMPANY THREE regularly offers reward or bounties to persons who will provide them cyber exploits. In or about September 2023, COMPANY THREE posted on its public-facing social media account that it would increase its bounty payouts from $200,000 to $20,000,000. In that same bounty, COMPANY THREE indicated that the exploits were for end users located in non-NATO countries.

15. Starting in at least April 2022, WILLIAMS created an email account with a foreign email provider under the pseudonym "John Taylor," and contacted COMPANY THREE through encrypted communication applications and the anonymized email account advertised on its bounty post. WILLIAMS did so to negotiate a price and contract to sell COMPANY THREE one of the Protected Products belonging to COMPANY ONE, namely Item 1, for his personal profit. WILLIAMS negotiated and signed a contract with COMPANY THREE using the John Taylor alias wherein he agreed to provide the trade secrets in Item 1 to COMPANY THREE for approximately $240,000. To complete the transfer, WILLIAMS first obtained the protected trade secrets for Item 1 by accessing COMPANY ONE's Secure Network, and then using a hard drive to transfer without authorization that data to a personal computer. He then removed identifying information specific to himself and/or COMPANY ONE and transmitted the secrets through encrypted applications and accounts designated by COMPANY THREE, in exchange for an initial payment. COMPANY THREE agreed to make additional payments under the contract once: (i) the software's performance

was confirmed; and (ii) whenever WILLIAMS subsequently updated the software to maintain its efficacy. WILLIAMS requested and obtained payment in cryptocurrency from COMPANY THREE.

16. Between April 2022 and June 2025 WILLIAMS was in regular communication with COMPANY THREE. Thereafter WILLIAMS entered into multiple written contracts with COMPANY THREE for the sale of at least seven additional trade-secret items belonging to COMPANY ONE, including trade secrets from Items 2 through 8. Each of these contracts had an upfront payment, depending on whether the exploit was successful, to be followed by additional payments if the item continued to function, and at least three months of follow-on support in exchange for an additional $10,000 per month.

17. In sum, WILLIAMS agreed to receive over $4,000,000 though these contracts, and he did receive upfront payments in the form of cryptocurrency from COMPANY THREE worth in excess of $1,300,000. As part of these contracts, WILLIAMS agreed to transfer the protected trade secrets from COMPANY ONE, including trade secrets contained in Items 1 through 8, such as the source code, to COMPANY THREE. In each case, WILLIAMS followed through on delivery of the secrets contained in Items 1 through 8. In each case, WILLIAMS bypassed COMPANY ONE's security protections; physically removed secrets from COMPANY ONE's Secure Network system both in the District of Columbia or in Sydney, Australia, using a portable hard drive; transferred the stolen secrets to a personal device; and then transferred the secrets to COMPANY THREE using encrypted means. One of these contracts involved a December 4, 2023, agreement in which WILLIAMS agreed to provide COMPANY THREE with trade secrets in Item 2 for $2,000,000. That agreement was consistent with a public bounty that COMPANY THREE published in September 2023. In another contract with COMPANY THREE, WILLIAMS agreed in June 2025 to provide COMPANY THREE with secrets in Item 8 for $500,000. WILLIAMS delivered Item 8

in July 2025, and agreed to receive a bulk payment of $300,000 that month and two additional payments of $100,000, with the last payment in September 2025. COMPANY THREE made a payment to WILLIAMS in cryptocurrency in July 2025, and WILLIAMS transferred that payment to one of his accounts in August 2025.

18. After obtaining payment from COMPANY THREE, WILLIAMS engaged in further transactions involving the proceeds of those payments. WILLIAMS used a virtual currency exchange that does not require users to create accounts and generally does not collect customer identifying information unless a specific transaction is flagged for further review. WILLIAMS also moved funds between different cryptocurrencies and blockchains. For example, WILLIAMS conducted multiple transfers of cryptocurrency proceeds before converting the proceeds into fiat currency which he deposited into accounts in Australia and the United States.

WILLIAMS's Cooperation After Being Confronted by Law Enforcement

19. In a voluntary interview with the FBI on August 6, 2025, WILLIAMS did not initially disclose any alias accounts or inculpatory information. Immediately thereafter, FBI agents confronted WILLIAMS with evidence of his criminal activity. WILLIAMS then admitted to his culpable conduct and his illicit activities. WILLIAMS described to law enforcement how he accomplished the theft of the trade secrets from COMPANY ONE's Secure Network from its offices in the District of Columbia and Australia as set forth in sum and substance in paragraphs 15 to 18 of this Statement of Offense. WILLIAMS admitted that he sold at least one trade secret even after he recognized code he wrote and sold to COMPANY THREE being utilized by a South Korean broker. WILLIAMS acknowledged that that he intentionally did not disclose his John Taylor email accounts when asked earlier during the interview. WILLIAMS expressed remorse and acknowledged that he had harmed the intelligence communities of Australia and the United

States.

20. WILLIAMS acknowledged that he liquidated the cryptocurrency proceeds he received from COMPANY THREE into local fiat currency and moved the money into his personal accounts. WILLIAMS also acknowledges that he used the proceeds from COMPANY THREE to purchase and pay the down payment for a house in Washington, D.C. in 2025 (further identified in the Information) and for the items identified in the Plea Agreement.

21. This statement is not intended to include all of the information known to the United States concerning the defendant, WILLIAMS. Rather, it is intended only to provide those facts necessary to establish a factual basis for WILLIAMS's plea of guilty to the offenses of Theft of Trade Secrets, in violation of 18 U.S.C. § 1832.

Respectfully submitted,
United States Attorney

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

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

DEFENDANT'S ACKNOWLEDGMENT

I have read and discussed this Proffer of Facts with my attorney. I agree and acknowledge by my signature that this Proffer of Facts is true and correct.

Date: 10/10/25

PETER WILLIAMS
Defendant

Date: 10/10/2025

JOHN P. ROWLEY III, ESQ.
Attorney for Defendant

Date: 10/10/2025

LIONEL ANDRE, ESQ.
Attorney for Defendant