**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| **v.** | : | **Case No: 21-CR-577 (CJN)** |
| **MARC BAIER,** | : | |
| **RYAN ADAMS, and** | : | |
| **DANIEL GERICKE,** | : | |
| **Defendants.** | : | |

## DEFERRED PROSECUTION AGREEMENT

Marc Baier, Ryan Adams, and Daniel Gericke (collectively, "defendants"), by their undersigned and authorized representatives, hereby enter into this Deferred Prosecution Agreement (the "Agreement") with the United States Attorney's Office for the District of Columbia and the United States Department of Justice, National Security Division (collectively, the "Offices").

### Criminal Information and Factual Statement

1. The defendants acknowledge and agree to the filing of a two-count criminal Information in the United States District Court for the District of Columbia (the "Information"), charging them with: (1) knowingly and willfully conspiring, in violation of Title 18, United States Code, Section 371, to violate the Arms Export Control Act ("AECA") and the International Traffic in Arms Regulations ("ITAR"); and (2) knowingly conspiring, in violation of Title 18, United States Code, Section 371, to commit access device fraud, and computer fraud and abuse, in violation of Title 18 United States Code, Sections 1029 and 1030. In so doing, the defendants: (a) knowingly waive their right to indictment on these charges, as well as all rights to a speedy trial pursuant to the Sixth Amendment of the United States Constitution, Title 18, United States Code,

Section 3161, Federal Rule of Criminal Procedure 48(b), and Local Criminal Rule 45.1 of the United States District Court for the District of Columbia; and (b) knowingly waive any objection with respect to venue to any charges by the Offices arising out of the conduct described in the Factual Statement attached hereto as Exhibit A (the "Factual Statement"), and consent to the filing of the Information in the United States District Court for the District of Columbia.

2. The defendants admit, accept, and acknowledge under oath that the facts and descriptions of their conduct, and that of persons working with and for them, as set forth in the Factual Statement are true and accurate. If the Offices, pursuant to Paragraph 31 of this Agreement, pursue a prosecution that is deferred by this Agreement, each of the defendants stipulates to the admissibility of the Factual Statement in any such proceeding, including any trial, guilty plea, appeal, civil or criminal forfeiture proceeding, or sentencing proceeding, and will not contradict anything in the Factual Statement at any such proceeding.

**Term of the Agreement**

3. This Agreement is effective for a three-year period beginning on the date on which the Information was filed, ending on September 14, 2024 (the "Term"). The defendants agree, however, that, in the event the Offices determine, in their sole discretion, that any of the defendants have knowingly violated any provision of this Agreement or have failed to completely perform or fulfill each of their obligations under this Agreement, an extension or extensions of the Term for the offending defendant may be imposed by the Offices, in their sole discretion, for up to a total additional time period of one year, without prejudice to the Offices' right to proceed as provided in Paragraph 31 below. Any extension of the Term of the Agreement extends all terms of this Agreement, for an equivalent period. Conversely, in the event the Offices find, in their sole discretion, that there exists a change in circumstances sufficient to eliminate the need for the

restrictions and requirements in Paragraphs 7—18, and that the other provisions of this Agreement have been satisfied, the Term of the Agreement may be terminated early.

4. The conditions discussed in Paragraphs 17—18 are not limited to the Term. The defendants agree to comply with those provisions even after the end of the Term.

**Definitions**

5. As used in this Agreement, the term Computer Network Attack ("CNA") includes the use of computers (including smart phones, mobile devices, and devices capable of connecting to the Internet or computer networks), computer networks, or electronic communications to disrupt, deny, degrade, delete, or destroy information resident in computers and computer networks, or the computers and networks themselves.

6. As used in this Agreement, the term Computer Network Exploitation ("CNE") includes the use of computers (including smart phones, mobile devices, and other devices capable of connecting to the Internet or computer networks), computer networks, or electronic communications to access, collect, scan, or retrieve the non-public contents of any computers or computer networks, without the user's authorization, as well as the use of computers, computer networks or electronic communications to view, copy, change, or otherwise interact with data on computers or computer networks without the users' authorization, including data saved on devices as well as data held by third-party storage providers.

**Restrictions, Cooperation, and Disclosure Requirements**

7. Within 60 days of this agreement, the defendants shall resign from any employment, consulting, teaching, contracting, or sub-contracting relationship with any and all United Arab Emirates (U.A.E.) intelligence, law enforcement, military, or defense entities and persons (including government agencies, officials, rulers, and their families), companies –

including subcontractors – with contracts with U.A.E. intelligence, law enforcement, military, or defense entities, and U.A.E. CO , , , , , and any associated, related, or successor entities.

8. The defendants shall cooperate fully with the Offices and meet with and provide full, complete, and truthful information to the FBI or any other U.S. government organization, upon request of the Federal Bureau of Investigation (FBI), including any follow-on meetings requested (the first meeting to occur within 90 days of signature of the agreement unless otherwise agreed to by the parties) at places and times to be determined by the FBI. This includes providing any documents, material, data, or information requested by the FBI that are in the possession or control of the defendants as of the time of the acceptance of this agreement. Cooperation does not require the defendants to waive their attorney-client or attorney-work product privileges. However, the defendants must provide to the Offices a log of any information or cooperation that is not provided based on an assertion of law, regulation, or privilege, and the defendants bear the burden of establishing the validity of any such assertion.

9. The defendants shall disclose to the Offices and FBI all tax returns (and related attachments) and identify all assets owned or controlled by themselves and their immediate family members, including property, bank accounts, virtual currency assets and wallets, and agreements to be paid monies (including IOUs, financial commitments, or promises of repayment or reimbursement), from 2016 to present. Following the initial disclosures, the defendants shall make annual disclosures by May 1 of each year during the Term.

10. The defendants shall inform the Offices of their current employment (including as employees, consultants, contractors, or sub-contractors) and any changes in such relationships, or change in ownership of the employer. The defendants shall obtain preapproval from the Offices

prior to obtaining or engaging in any employment that would involve the defendants engaging in, advising about, consulting about, training or teaching CNA and CNE techniques, as well as any employment regarding the support of CNA and CNE activities (including, but not limited to, software or malware development, infrastructure development, operations management, targeting techniques, cryptology, and data analysis). For the purposes of this Paragraph, "employment" shall also include the retention or engagement of defendants by anyone for any duration of time, in exchange for compensation, including but not limited to speaking engagements, presentations at conferences, writing contracts, memoirs, book/movie deals, or training sessions.

11. For activities other than those covered by paragraph 10, the defendants shall provide at least 30 days' notice to the FBI Cyber Division CYWATCH (24/7 number: 1-855-292-3937 or email CyWatch at cywatch@fbi.gov) prior to seeking or accepting (whichever comes first) any paid or unpaid employment, consultancy, teaching or subcontracting relationship for the benefit of a foreign government, or for an organization that contracts or subcontracts with a foreign country's intelligence, law enforcement, military or defense services.

12. The defendants shall not engage in any employment (including as employees, consultants, contractors, or subcontractors) that would involve the defendants exporting any defense articles or providing any defense services under the ITAR, including but not limited to, any defense services involving CNA or CNE techniques.

13. The defendants agree during the Term to comply with all U.S. statutes and regulations related to the monitoring of foreign agents, including all requirements of 18 U.S.C. Chapter 45 (Foreign Relations), 22 U.S.C. § 611 et seq., and 50 U.S.C. § 851.

14. The defendants shall immediately relinquish any U.S. government security clearances and shall inform the relevant agencies about this Agreement.

15. The defendants shall immediately relinquish any U.A.E. government security clearances and defendants shall provide at least 30 days' notice to the FBI Cyber Division CYWATCH (24/7 number: 1-855-292-3937 or email CyWatch cywatch@fbi.gov) prior to obtaining any security clearances from any foreign governments.

16. The defendants understand and agree that upon filing of the Information, they will need to be formally booked by law enforcement entities. If requested by the defendants, the Offices will seek Court approval to conduct such booking procedures at the U.S. Embassy in the U.A.E.

**Other Assurances**

17. The defendants agree to never knowingly solicit employment from, or work for, in any capacity (i.e., as employees, consultants, teachers, contractors, or subcontractors) any U.A.E. government organization (including but not limited to any agency, bureau, department, office, or program) with responsibility for law enforcement, national security, intelligence, armed forces, or defense services. This prohibition includes any private entity that is a provider of CNA or CNE services (whether as a contractor or subcontractor) to any such U.A.E. government organization, including but not limited to U.A.E. CO [redacted], [redacted], [redacted], [redacted], [redacted], or any associated, related, or successor entities. The defendants agree that if a defendant violates this provision after the expiration of the Term, the violating defendant will agree to forfeit and pay liquidated damages to the United States in the amount of their full compensation from such employment, payable on the 1st day of January of each subsequent year.

18. The defendants agree to never seek or obtain a U.S. government security clearance.

**Payment of Monetary Penalty**

19. The Offices and the defendants agree that, if the defendants were convicted of the criminal violations set forth in the Information, they could be sentenced to pay a fine in accordance with Title 18, United States Code, Sections 3571(d) and 3572(a). In addition, the Offices and the defendants agree that, as a result of the conduct set forth in the Factual Statement, the Offices could institute a civil and/or criminal forfeiture action against certain funds and/or property of the defendants and that such funds and/or property would be forfeitable pursuant to Title 18, United States Code, Sections 981 and/or 982. In lieu of a criminal prosecution and sentence or fine, or a civil or criminal forfeiture action, the Offices and the defendants agree that a monetary penalty based on the total amount they earned as employees of U.A.E. CO or its successor entities is appropriate in this case (the "Monetary Penalty"). The Monetary Penalty shall be paid as follows: seven hundred and fifty thousand U.S. dollars ($750,000) by defendant Baier, six hundred thousand U.S. dollars ($600,000) by defendant Adams, and three hundred and thirty five thousand U.S. dollars ($335,000) by defendant Gericke. Each of the defendants, and the Offices, agree that the Monetary Penalty is appropriate given the facts and circumstances of this case, including the nature and seriousness of the conduct. Any payments made toward satisfaction of the Monetary Penalty are final and shall not be refunded. Furthermore, nothing in this Agreement shall be deemed an agreement by the Offices that the Monetary Penalty is the maximum fine that may be imposed in any future prosecution, and the Offices are not precluded from arguing in any future prosecution that the Court should impose a higher fine, although the Offices agree that under those circumstances, it will recommend to the Court that any amount paid under this Agreement should be offset against any fine the Court imposes as part of a future judgment relating to the conduct

described in the Factual Statement. The defendants acknowledge that no tax deduction may be sought in connection with the payment of any part of the Monetary Penalty.

20. The defendants each agree that payment of their respective portion of the Monetary Penalty, plus any associated transfer fees, shall be made by wire transfer pursuant to instructions provided by the Offices via full payment at once, or in equal installment payments to be made every 90 calendar days (greater or accelerated payments are also permissible), with the first payment due within 90 calendar days of the execution date of the Agreement and the final payment due 90 calendar days prior to the last day of the Term. The defendants agree to release any and all claims they may have to such funds, and further certify that each passes clean title to these funds, which are not the subject of any lien, security agreement or other encumbrance. Transferring encumbered funds or failing to pass clean title to the funds in any way will be considered a breach of this agreement. The defendants shall indemnify the Offices for any costs it incurs associated with the passing of clean title to the funds.

21. In the event that the United States Department of State ("DOS") or the Directorate of Defense Trade Controls ("DDTC") levies, institutes, charges, or issues any fines or penalties against a defendant for the conduct described in the Factual Statement (e.g., a fine or penalty based administrative or civil violations of law), the Monetary Penalty amounts for that defendant shall be reduced by the amount of DOS and/or DDTC fine or penalty paid by that defendant.

22. No monies owed by the defendants under this Agreement can be reimbursed or paid directly, or indirectly, by any other person or entity, including but not limited to any U.A.E. government entity or person (including agencies, officials, rulers, and their families), companies – including subcontractors – with contracts with a U.A.E. government entity, and U.A.E. CO

[redacted], [redacted], [redacted], [redacted], [redacted], and any associated, related, or successor entities, without prior consent of the Offices.

**Conditional Release from Liability**

23. Subject to Paragraphs 29—36, the Offices agree, except as provided in this Agreement, that they shall not seek to prosecute the defendants for any act specified in the Factual Statement or taken in furtherance of the offenses charged in the Information. The Offices, however, may use any information related to the conduct described in the Statement of Facts against the defendants: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code

24. This Agreement does not provide any protection for any other criminal or civil matter.

25. This Agreement does not provide any protection against prosecution for any future conduct by the defendants.

26. This Agreement does not provide any protection against any prosecution of any other individuals, regardless of their affiliation with the defendants.

27. Absent a Breach, with respect to any prosecution that may be brought against defendants by the Offices, the Offices will not offer in evidence in its case-in-chief any statements made by defendants during interview(s) or testimony given as part of defendants' obligations under this Agreement or the statements in the Statement of Facts.

28. Notwithstanding Paragraph 27 above, the Offices may: (a) use all information derived directly or indirectly from defendants' interview(s) for the purpose of obtaining and

pursuing leads to other evidence, which evidence may be used for any purpose, including any prosecution of the defendants; and (b) use statements made by defendants pursuant to their interview(s) and all evidence obtained directly or indirectly from those statements for the purpose of cross-examination should defendants testify, or to refute or counter at any stage of a criminal proceeding any evidence, argument, statement or representation offered by or on behalf of defendants in connection with any proceeding.

**Deferral of Prosecution**

29. In consideration of the undertakings agreed to by the defendants herein, including (a) past and future cooperation as described herein; (b) various restrictions described herein to demonstrate the defendants' good conduct; and (c) payment of a monetary penalty agreed to by the defendants herein, the Offices agree that any prosecution of the defendants for the conduct set forth in the Factual Statement and the Information be and hereby is deferred for the Term of this Agreement.

30. The Offices further agree that if any of the defendants fully comply with all of their obligations under this Agreement, the Offices will not continue the criminal prosecution against those fully compliant defendants described in Paragraph 1 and, at the conclusion of this Term, the Agreement shall expire. Within 30 days of the expiration of the Term of this Agreement set forth above in Paragraph 3 (including any extension as discussed therein), or less at the discretion of the Offices, the Offices shall seek dismissal with prejudice of the Information filed against those compliant defendants described in Paragraph 1, and agree not to file charges in the future against those defendants based on the conduct described in this Agreement and the attached Factual Statement.

## Breach of the Agreement

31. If, during the Term, any defendant: (a) commits any felony under United States federal law; (b) provides in connection with this Agreement intentionally false, incomplete, or misleading information; (c) knowingly and materially fails to cooperate as set forth in Paragraphs 7—20 of this Agreement; or (d) otherwise knowingly and materially fails to completely perform or fulfill each of his obligations under the Agreement, that defendant shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited to, the charges in the Information described in Paragraph 1, which may be pursued by the Offices in the United States District Court for the District of Columbia, or any other appropriate venue. Determination of whether a defendant has knowingly and materially breached the Agreement and whether to pursue prosecution shall be in the Offices' sole discretion. Any such prosecution relating to the conduct described in the attached Factual Statement or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement, subject to any tolling agreements between the Offices and the defendants, may be commenced against the defendants, notwithstanding the expiration of the statute of limitations, between the execution date of this Agreement and the expiration of the Term plus one (1) year. Thus, by signing this Agreement, each of the defendants agree that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term plus one year. In addition, the defendants agree that the statute of limitations as to any violation of federal law that occurs during the Term will be tolled from the date upon which the violation occurs until the earlier of the date upon which the Offices are made aware of

the violation or the duration of the Term, plus one year, and that this period shall be excluded from any calculation of time for purposes of the application of the statute of limitations.

32. If the Offices determine that any of the defendants has knowingly and materially breached any provision of this Agreement, the Offices shall provide written notice to that defendant's counsel of the alleged breach prior to instituting any prosecution resulting from such breach. Within 30 days of receipt of such notice, that defendant shall have the opportunity to respond to the Offices in writing to explain the nature, materiality, and circumstances of such breach, as well as the actions the defendant has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to pursue prosecution of that defendant.

33. In the event that the Offices determine that a defendant has knowingly and materially breached this Agreement: (a) all statements made by or on behalf of the defendants to the Offices or to the Court, including the attached Factual Statement, all statements made by the defendants to the FBI (including during the Term), and any testimony given by the defendants before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against any of the defendants; and (b) the defendant shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the defendant prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible.

34. The defendants also understand that the Offices reserve the right to criminally charge them with new violations of law based on future conduct, including during the Term, and that they may be charged with false statements and obstruction of justice should they provide false or fictitious information to the Government under this Agreement. The defendants further agree not to claim at any time that finding breach of this Agreement is the Government's sole remedy for future conduct that also violates the terms of this Agreement.

35. In the event of a knowing and material breach of this Agreement resulting in a prosecution for the charges contained in the Criminal Information and any other charges related to the conduct described in the Factual Statement, each of the defendants agrees to waive any and all extradition and removal proceedings to the United States from any foreign country (even if the country has no extradition treaty with the United States).

36. The defendants acknowledge that the Offices have made no representations, assurances, or promises concerning what sentence may be imposed by the Court if any of the defendants knowingly and materially breach this Agreement and the matter proceeds to judgment. The defendants further acknowledge that any such sentence is solely within the discretion of the Court and that nothing in this Agreement binds or restricts the Court in the exercise of such discretion.

**Public Filing**

37. The defendants and the Offices agree that this Agreement (and all attachments) shall be publicly filed in the United States District Court for the District of Columbia.

**Public Statements by the Defendants**

38. The defendants expressly agree that none of them shall themselves, or through other representatives, including present or future attorneys, make any public statement, in litigation or

otherwise, contradicting the facts described in the attached Factual Statement. Any such contradictory statement shall constitute a breach of this Agreement, and the defendants thereafter shall be subject to prosecution as set forth in Paragraph 28 of this Agreement. The decision of whether any public statement by any such person contradicting the facts described in the Factual Statement has occurred shall be in the sole discretion of the Offices. If the Offices determine that a public statement by any such person contradicts, in whole or in part, a statement contained in the Factual Statement, the Offices shall so notify that defendant, that defendant may avoid a breach of this Agreement by publicly repudiating such statement within five (5) business days after notification. The defendants shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Factual Statement provided that such defenses and claims do not contradict, in whole or in part, a statement contained in the Factual Statement.

**Other Conditions and Consequences**

39. This Agreement is conditioned on the acceptance of the Agreement by all of the defendants. If any of the defendants fails to accept the Agreement, the Government may revoke this Agreement, withdraw or void the Agreement against any or all defendants (at its sole option), or dismiss any proceeding instituted pursuant to this Agreement, at the option of the Government.

**Limitations on Binding Effect of Agreement**

40. This Agreement is binding on the defendants and the Offices, but specifically does not bind any other component of the United States Department of Justice, other federal agencies, or any state, local or foreign agencies, or any other authorities, although the Offices will bring the defendants' cooperation and compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so. Nothing in this Agreement restricts

in any way the ability of any other federal department or agency, or any state or local government from proceeding criminally, civilly, or administratively, against the defendants.

**Notice**

41. Any notice to the Offices under this Agreement shall be given by personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail addressed to:

U.S. Department of Justice
National Security Division
Counterintelligence & Export Control Section
950 Pennsylvania Avenue NW
Washington, D.C. 20530

with copy to:

United States Attorney
U.S. Attorney's Office for the District of Columbia
555 4th Street NW
Washington, D.C. 20530

Any notice to the defendants under this Agreement shall be given by personal delivery, overnight delivery by recognized delivery service, or registered or certified mail addressed to:

Marc Baier
c/o Kenneth L. Wainstein, Esq.
Davis, Polk & Wardwell LLP
901 15th Street, N.W.
Washington, D.C. 20005

Ryan Adams
c/o Thomas G. Connolly, Esq.
Harris, Wiltshire & Grannis LLP
1919 M Street, N.W.
Washington, D.C. 20036

Daniel Gericke
c/o Michael S. Dry
Vinson & Elkins LLP
2200 Pennsylvania Ave., NW Suite 500W
Washington, D.C. 20037

Notice shall be effective upon actual receipt by the Offices or the defendants' counsel.

**Exhibits**

42. Any and all exhibits to this Agreement are integral parts of the Agreement and are incorporated into this Agreement as though fully set forth in the Agreement.

**Execution in Counterparts**

43. This Agreement may be executed in one or more counterparts, each of which shall be considered effective as an original signature. Further, all facsimile and digital images of signatures shall be treated as originals for all purposes. The execution date shall be the last date when all signatories have signed the Agreement.

**Complete Agreement**

44. This Agreement, including all exhibits or attachments, sets forth all the terms of the Agreement between the defendants and the Offices. There are no promises, agreements, or conditions that have been entered into other than those expressly set forth in this Agreement, and none shall be entered into and/or be binding upon the defendants or the Offices unless signed by the Offices, or the defendant's attorney. This Agreement supersedes any prior promises, agreements, or conditions between any of the defendants and the Offices. The defendants agree to abide by all terms and obligations of this Agreement as described herein. No amendments, modifications or additions to this Agreement shall be valid unless they are in writing and signed by the Offices, and the attorneys for the defendants.

**AGREED:**

Date: 7 SEPTEMBER 2021 By: _____
Marc Baier

Date: September 7, 2021 By: _____
Kenneth Wainstein, Esq.
Davis, Polk & Wardwell LLP

Date: _____ By: _____
Ryan Adams

Date: _____ By: _____
Thomas G. Connolly, Esq.
Harris, Wiltshire & Grannis LLP

Date: _____ By: _____
Daniel Gericke

Date: _____ By: _____
Michael S. Dry, Esq.
Vinson & Elkins LLP

**AGREED:**

Date: _____ By: _____
Marc Baier

Date: _____ By: _____
Kenneth Wainstein, Esq.
Davis, Polk & Wardwell LLP

Date: 2021-09-07 By: _____
Ryan Adams

Date: 2021-09-07 By: _____
Thomas G. Connolly, Esq.
Harris, Wiltshire & Grannis LLP

Date: _____ By: _____
Daniel Gericke

Date: _____ By: _____
Michael S. Dry, Esq.
Vinson & Elkins LLP

**AGREED:**

Date: _____ By: _____
Marc Baier

Date: _____ By: _____
Kenneth Wainstein, Esq.
Davis, Polk & Wardwell LLP

Date: _____ By: _____
Ryan Adams

Date: _____ By: _____
Thomas G. Connolly, Esq.
Harris, Wiltshire & Grannis LLP

Date: 9/7/2021 By: _____
Daniel Gericke

Date: 9/7/2021 By: _____
Michael S. Dry, Esq.
Vinson & Elkins LLP

**FOR THE U.S. DEPARTMENT OF JUSTICE:**

CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY
FOR THE DISTRICT OF COLUMBIA

9/14/2021
DATE

By: _____
Tejpal S. Chawla
Demian Ahn
Assistant United States Attorneys

MARK J. LESKO
ACTING ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

9/14/2021
DATE

By: _____
Ali Ahmad
Counsel for Cyber Investigations
Scott Claffee
Trial Attorney
Counterintelligence & Export Control Section

***Exhibit A***

Factual Statement

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| **v.** | : | **Case No: _____** |
| **MARC BAIER,** | : | |
| **RYAN ADAMS, and** | : | |
| **DANIEL GERICKE,** | : | |
| **Defendants.** | : | |

## FACTUAL STATEMENT

This Factual Statement is made pursuant to, and is part of, the Deferred Prosecution Agreement ("DPA") dated September 7th, 2021, between the United States Attorney's Office for the District of Columbia, the United States Department of Justice, National Security Division (collectively, "DOJ") and Marc Baier, Ryan Adams and Daniel Gericke (collectively, "Defendants").[1] Defendants agree and stipulate that, in the event DOJ brings a deferred prosecution pursuant to the DPA (the "prosecution"): the information in this Factual Statement is true and accurate; this Factual Statement is admissible for all purposes related to the prosecution; and they will neither contest the admissibility of, nor contradict any factual assertions contained in, this Factual Statement. The parties further agree that, although each defendant individually may not have contemporaneously known all of the facts and events described in this Factual Statement, the Factual Statement correctly describes the facts and events described herein, and that the facts and events discussed in this Factual Statement occurred on or about the dates described.

[1] Unless stated otherwise, the phrase "Defendants" refers to and includes all three Defendants.

## Introduction

1. Starting in or about December 2015 and continuing through at least November 2019, a company based in the United Arab Emirates ("U.A.E. CO") hired numerous non-U.A.E. nationals, including U.S. persons such as Defendants, to provide computer network services, including computer network exploitation ("CNE") services that included the development, maintenance, deployment, and operation of software and hardware designed to obtain unauthorized access to electronic devices and accounts. Defendants, as well as others who were supervised, supported, aided, and abetted by Defendants, used their expertise to provide and support CNE services at U.A.E. CO for the benefit of a U.A.E. government agency ("U.A.E. AGENCY ONE") and a successor U.A.E. government agency ("U.A.E. AGENCY TWO"). The systems developed, maintained, deployed, and operated by Defendants allowed U.A.E. CO to gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers around the world, including on computers and servers in the United States, as well as computers and servers that communicated with computers in the United States and were connected to and part of the Internet, in support of the U.A.E.'s intelligence gathering efforts. In addition, at least one of the CNE systems developed and deployed by Defendants was a defense article as defined by U.S. export control regulations, and Defendants did not obtain the required authorization from the U.S. government to provide defense services to foreign persons in connection with any such articles.

## The Arms Export Control Act and International Traffic in Arms Regulations

2. In furtherance of the national security and foreign policy interests of the United States, the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778, regulates and restricts the sale of arms, munitions, implements of war, and other defense articles and services.

3. Pursuant to the authority granted in the AECA, the U.S. Department of State promulgated the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. The ITAR governs the export of "defense articles" and the provision of "defense services."

4. The list of controlled defense articles is contained in the United States Munitions List ("USML"), 22 C.F.R. § 121.1, which designates certain items and related technical data as "defense articles." The USML is composed of various categories of items, systems, equipment, parts, components, accessories, attachments, and technical data and defense services related to defense articles.

5. Category XI(b) of the USML designates as a defense article "Electronic systems, equipment or software, not elsewhere enumerated . . . , specially designed for intelligence purposes that collect, survey, monitor, or exploit, or analyze and produce information from, the electromagnetic spectrum (regardless of transmission medium), or for counteracting such activities." 22 C.F.R. § 121.1. A "system" is defined as "a combination of parts, components, accessories, attachments, firmware, software, equipment, or end-items that operate together to perform a function." 22 C.F.R. § 120.45(g).

6. "Defense services," as that term is used in 22 U.S.C. § 2778(b)(2) and the ITAR, means, in relevant part:

> (1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; [or]
>
> (2) The furnishing to foreign persons of any technical data controlled under [the ITAR], whether in the United States or abroad[.]

22 C.F.R. § 120.9(a)(1)–(2).

7. The ITAR further recognizes that before a U.S. person can furnish a "defense service" to a foreign person he/she must apply to the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC") for a either a specific license for each service he/she wishes to provide, or for a license and Technical Assistance Agreement ("TAA") that can cover various types of services allowing TAA-covered parties to avoid individualized licensing review for each ITAR-covered service. 22 C.F.R. § 124.1.

8. Accordingly, U.S. persons seeking to provide "defense services" to persons outside the United States must obtain a license or other approval, or must be employed by a company who has obtained a license or other approval, from DDTC, which is located in the District of Columbia.

9. The AECA makes it a crime for any person to "willfully violate[] any provision [of the AECA] . . . or any rule or regulation issued under [the AECA]," including the ITAR. 22 U.S.C. § 2778(c). Pursuant to the ITAR, it is unlawful, without approval from DDTC, to: "furnish or attempt to furnish any defense service," 22 C.F.R. § 127.1(a)(1); "reexport or retransfer or attempt to reexport or retransfer any defense article, technical data, or defense service from one foreign end-user, end-use, or destination to another foreign end-user, end-use, or destination," *id*. § 127.1(a)(2); "conspire to export, import, reexport, retransfer, furnish or cause to be exported, imported, reexported, retransferred or furnished, any defense article, technical data, or defense service for which a license or written approval is required by this subchapter," *id*. § 127.1(a)(4); and, "violate any of the terms or conditions of a license or approval granted pursuant to this subchapter, any exemption contained in this subchapter, or any rule or regulation contained in this subchapter." *Id*. § 127.1(b)(1).

10. The ITAR also states that "[n]o person may knowingly or willfully attempt, solicit, cause, or aid, abet, counsel, demand, induce, procure, or permit the commission of any act

prohibited by, or the omission of any act required by 22 U.S.C. § 2778, 22 U.S.C. § 2779, or any regulation, license, approval, or order issued thereunder." 22 C.F.R. § 127.1(e).

**Computer Fraud and Access Device Fraud**

11. The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, prohibits, among other things, using unauthorized access to a protected computer to obtain information, *id*. § 1030(a)(2), and knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer, *id*. § 1030(a)(5)(A).

12. Under the CFAA, a "protected computer" is any computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

13. It is a crime to knowingly, and with intent to defraud, use one or more unauthorized access devices during any one year period, and by such conduct obtain a thing of value in excess of $1,000. 18 U.S.C. § 1029(a)(2). It is likewise a crime to knowingly, and with intent to defraud, possess fifteen or more unauthorized access devices. *Id*. § 1029(a)(3). The term "access device" includes "any . . . code, account number, . . . or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." *Id*. § 1029(e)(1).

## The Defendants and Relevant Entities

14. U.S. COMPANY ONE was a U.S.-based company that, during the relevant time period, employed U.S. persons and provided cyber services, including training and support, to the U.A.E. government pursuant to TAAs and other licenses authorized by DDTC under the ITAR.

15. U.A.E. CO was a privately held technology and cyber services company headquartered and organized in the U.A.E and was a competitor of U.S. COMPANY ONE for the provision of cyber services to the U.A.E government. U.A.E. CO, together with its subsidiaries and related companies, and related successor companies, had offices in several countries and employed persons from around the world, including U.S. persons. During the relevant time period, U.A.E. CO provided staffing to the U.A.E. government, and U.A.E. CO personnel in turn provided the U.A.E. government with CNE services and related support activities, as well as more general cyber services.

16. Defendant MARC BAIER is a U.S. citizen and a former member of the U.S. armed forces who previously held a U.S. security clearance. BAIER also is a former employee of the U.S. Intelligence Community ("USIC"). Between 2012 and 2015, BAIER served in several roles that culminated in the position of General Manager of Middle East and North Africa programs for U.S. COMPANY ONE. In or about October 2015, BAIER agreed to join U.A.E. CO as a senior manager. Subsequently, between January 2016 and November 2019, BAIER was a U.A.E. CO executive and served, at various times, as a lead manager for CNE operations. In addition, BAIER sometimes advised senior U.A.E. government officials on CNE operations.

17. Defendant RYAN ADAMS is a U.S. citizen and a former member of the U.S. armed forces who previously held a U.S. security clearance. While serving in the U.S. armed forces, Adams worked within the USIC. Between 2010 and 2014, ADAMS was a U.S.

COMPANY ONE senior software engineer for certain cyber services. From 2014 to 2015, ADAMS was a mission director and manager at U.S. COMPANY ONE. In or about October 2015, ADAMS agreed to join U.A.E. CO working in the same capacity. Subsequently, between January 2016 and November 2019, ADAMS held various roles within U.A.E. CO, including in a managerial capacity, supporting CNE operations and related services.

18. Defendant DANIEL GERICKE was a U.S. citizen until February 2017 and previously held a U.S. security clearance. GERICKE is also a former member of the U.S. military, although GERICKE never worked within the USIC. Between 2013 and December 2015, GERICKE was a U.S. COMPANY ONE project leader for certain aspects of cyber services. In or about October 2015, GERICKE agreed to join U.A.E. CO as a manager for CNE operations. Subsequently, between January 2016 and late 2018, GERICKE held various roles within U.A.E. CO, including in a managerial capacity, supporting CNE operations and related services.

**Background on U.S. COMPANY ONE's Work for the U.A.E. Government**

19. Between about 2009 and about February 2016, U.S. COMPANY ONE provided cyber services, including training and support, to U.A.E. AGENCY ONE. Because the services provided by U.S. COMPANY ONE included defense services regulated by the AECA and the ITAR, U.S. COMPANY ONE provided those services pursuant to DDTC-approved licenses and TAAs.

20. DDTC approved U.S. COMPANY ONE's licenses and TAAs based upon representations made by all parties to the TAAs, which included authorized representatives of U.S. COMPANY ONE, U.A.E. AGENCY ONE, the U.A.E. government, and other related parties. The TAAs confirmed that all signing parties, including U.S. COMPANY ONE, U.A.E. AGENCY ONE, and the U.A.E. government, understood and agreed that U.S. COMPANY ONE was

providing defense services under to the ITAR to U.A.E. AGENCY ONE. Moreover, the last TAA, signed in 2014, stated that all parties would abide by U.S. export control laws and would not "target or exploit U.S. Persons (i.e., U.S. citizens, permanent resident aliens, or U.S. companies or entities, or other persons in the United States) . . . ." The TAAs also prohibited the parties and their employees from re-exporting or retransferring goods, services, information and data to third parties without prior consent from the U.S. State Department. Finally, the 2014 TAA required preapproval from a U.S. government agency prior to the release of "any presentations and/or content pertaining to cryptographic analysis and/or computer network exploitation or attack."

21. One of U.S. COMPANY ONE's U.A.E. contracts was codenamed "Raven." Many of U.S. COMPANY ONE's employees working on the Raven contract, known as the "Raven Team," were former USIC employees and some had active U.S. security clearances or had previously held active security clearances, including the Defendants. The Raven Team in the U.A.E. worked in secure facilities and operated independently of other U.S. COMPANY ONE employees who provided defensive cyber services to the U.A.E. government. Under the TAA, U.S. COMPANY ONE Raven Team employees provided training and operational support to U.A.E. AGENCY ONE.

22. Defendants, as Raven Team members and managers, were required to receive periodic TAA and ITAR trainings that indicated their work for U.A.E. AGENCY ONE and the U.A.E. was covered by the ITAR, and that they needed to remain in compliance with the TAA to lawfully provide the contracted CNE services to the U.A.E.

23. Between in or about December 2015 and February 2016, the U.A.E. government transitioned its contracts for cyber services from U.S. COMPANY ONE to a competitor, U.A.E.

CO. At no time did any of the Defendants, or U.A.E. CO, obtain a TAA or other export license from DDTC to provide defense services for U.A.E. CO or the U.A.E. government.

**Background on U.A.E. CO's Work for the U.A.E. Government**

24. Between about January 2016 and about November 2019, Defendants and U.A.E. CO provided the U.A.E. government, including U.A.E. AGENCY ONE and U.A.E. AGENCY TWO, with various cyber services, including CNE services and related support activities, as well as more general cyber services. Prior to hiring former employees of U.S. COMPANY ONE, U.A.E. CO did not have sufficient CNE experience or expertise to engage in CNE activity. Accordingly, U.A.E. CO obtained that CNE expertise, in part, by hiring key U.S. person managers of U.S. COMPANY ONE who worked on the Raven Team, including Defendants. U.A.E. CO offered these managers higher compensation packages to those they had received from U.S. COMPANY ONE. The U.S. person managers who accepted employment, including Defendants, became the founding members of a Raven Team successor at U.A.E. CO. This Raven Team successor group, *i.e.*, the non-U.A.E. employees within U.A.E. CO, was referred to as Cyber Intelligence-Operations ("CIO"). When the CIO entity was created, its employees, including Defendants, existed and operated in the same building, with the same terminals, setup and computer infrastructure, from which they operated under U.S. COMPANY ONE. The combination of the CIO group with the other U.A.E. persons working for U.A.E. AGENCY ONE and/or U.A.E. AGENCY TWO who worked with CIO in their building, is referred to here as U.A.E. CO CIO.

25. Starting in or about January 2016, BAIER became the senior U.S. executive of U.A.E. CO CIO. Between in or about January 2016 and October 2017, and between in or about Spring 2018 until November 2019, BAIER was Executive Cybersecurity Adviser at U.A.E. CO

CIO, and the lead manager for the U.S. person employees of U.A.E. CO CIO. As Executive Cybersecurity Adviser, BAIER advised executives at U.A.E. CO and his duties included consulting with U.A.E. AGENCY TWO leadership, receiving orders and taskings from U.A.E. AGENCY TWO and relaying updates to U.A.E. AGENCY TWO, assisting in creating and implementing CIO's strategic vision, managing U.A.E. CO CIO employees, overseeing CNE product acquisition and development, and supervising CIO's operations (including exploitation, collection of exfiltrated information, and development of CNE tools).

26. In January 2016, ADAMS was Director of Cyber Operations, and he remained in that position until in or about October 2016. As director of cyber operations at U.A.E. CO CIO, ADAMS' duties included briefing U.A.E. AGENCY TWO leadership on the implementation of CNE operations against targets approved by U.A.E. AGENCY TWO, supporting the development and integration of CNE tools, managing CIO's operations, and assisting BAIER. After December 2016, ADAMS moved to various different roles supporting CIO until October 2017. ADAMS was not directly involved with the CNE operations described in the Factual Statement after October 2017. Having migrated out of the CIO operations department entirely in approximately December 2017, ADAMS is unaware of CIO operations after that date.

27. In or about January 2016, GERICKE became a supervisor in U.A.E. CO CIO Operations. In that position, GERICKE was directly involved in CNE operations. In or about December 2016, GERICKE was promoted to lead teams within U.A.E. CO CIO Operations. Further, between October 2017 and January 2018, GERICKE was Program Manager of U.A.E. CO CIO, and supervised the development of CNE exploitation tools and collection. In about November 2018, GERICKE left CIO operations, but remained in the employment of U.A.E.CO.

28. CIO was principally dedicated to conducting CNE operations, as well providing all manner of support for CNE operations, on behalf of and for U.A.E. government agencies. The CNE services conducted by CIO provided access to information and data from thousands of targets around the world, and involved the following services:

(a) the acquisition, integration, and development of computer exploits from the United States and elsewhere;

(b) the acquisition, development, and deployment of customized systems and infrastructure to support CNE activities, including anonymizing software, servers, and hardware systems;

(c) accessing, without authorization, computers around the world to obtain information, through the transmission of information, computer code, and commands that traveled in and through the United States and elsewhere;

(d) causing damage to computers around the world through the transmission of information, computer code, and commands that traveled in and through the United States and elsewhere that allowed CIO to access those computers without authorization, for the purpose of obtaining information from those computers;

(e) collecting exfiltrated data from exploited devices, computers, and servers, and passing such data to CIO and U.A.E. government agencies, for further analysis;

(f) obtaining, possessing, and using means of identification and authentication features (*i.e.*, usernames, passwords, and other means of authentication) that were acquired without authorization and that were issued, managed, or controlled by providers organized under the laws of the United States; and,

(g) using computers to analyze and, as necessary, decrypt exfiltrated data.

**Defendants' Roles in U.A.E. CO CIO's Conduct**

29. Between January 2016 and November 2019 (the "Period"), Defendants and CIO personnel, including other former employees, and managers of U.S. COMPANY ONE, conducted, managed, supported, and directed CIO's CNE operations and related services. As noted above, Baier was involved with CIO between January 2016 and November 2019; Gericke was involved with CIO between January 2016 and November 2018; and Adams was involved with CIO between January 2016 and December 2017.

30. U.A.E. CO also recruited and hired persons from around the world (including other U.S. persons, as well non-U.S. and non-U.A.E. persons) to augment CIO. Defendants, as managers of U.A.E. CO during the Period, participated in the recruitment, interviewing, and hiring of new employees into U.A.E. CO CIO. Although Defendants had previously provided services pursuant to U.S. COMPANY ONE's TAA and licenses, none of the CIO personnel, including Defendants, sought or obtained authorization from the U.S. government to provide the same type of services that were provided by U.S. COMPANY ONE, including CNE services, to the U.A.E. government and did not apply for, or receive, a U.S. export license or TAA from the DDTC to provide defense services to the U.A.E. during the Period.

31. Before Defendants joined U.A.E. CO in 2016, U.S. COMPANY ONE told Defendants that U.S. persons could not lawfully support U.A.E. AGENCY ONE's intended CNE operations and related services under U.A.E. CO without obtaining a TAA or other authorization from DDTC.

32. Thereafter, in December 2015 and February 2016, U.S. COMPANY ONE, through employees and legal counsel, in writing and orally, advised Defendants and other U.S. COMPANY ONE employees and managers that U.S. COMPANY ONE's legal counsel had confirmed that

U.S. COMPANY ONE's existing TAA prohibited U.S. COMPANY ONE and its employees from sharing TAA-protected information and material with U.A.E. CO and its employees, that supporting U.A.E. CO's CNE operations and related services would constitute "defense services" under the ITAR, and that U.S. persons could not lawfully provide such services to foreign entities without a TAA or license from DDTC. U.S. COMPANY ONE, through employees and legal counsel, also informed Defendants that if they joined U.A.E. CO: (a) they would no longer be working under U.S. COMPANY ONE's TAA; (b) they would need their own TAA or license from DDTC to continue to provide the defense services they had been previously providing to the U.A.E. government under U.S. COMPANY ONE's TAA; and (c) they could not access or distribute U.S. COMPANY ONE's TAA-restricted information without preapproval, as required by U.S. COMPANY ONE's TAA.

33. Defendants did not seek or obtain any contradictory legal advice on these matters from individual legal counsel or from U.A.E. CO.'s in-house legal counsel, although Defendants were aware that U.A.E. CO's in-house legal counsel was involved in discussions concerning legal issues related to the transition from U.S. COMPANY ONE to U.A.E. CO. U.A.E. CO's in-house legal counsel did not provide Defendants with any advice or warnings concerning the ITAR.

34. U.S. COMPANY ONE terminated Defendants' employment at their or the U.A.E.'s request, effective December 31, 2015, and they thereafter became U.A.E. CO managers working at the same location and in their same capacity. Defendants were aware that U.A.E. CO hired them and their former U.S. COMPANY ONE coworkers to provide the same CNE operations and related services for intelligence purposes to the U.A.E. government, including U.A.E. AGENCY ONE and U.A.E. AGENCY TWO, on behalf of U.A.E. CO.

35. After Defendants moved to work for U.A.E. CO, they recruited U.S. COMPANY ONE employees to join them at U.A.E. CO and continue providing CNE services to U.A.E. AGENCY ONE. Each of the Defendants told one or more U.S. COMPANY ONE employees that the benefits to moving to U.A.E. CO included generally higher compensation packages than what they had earned at U.S. COMPANY ONE and an expanded budget for CNE operations.

36. In January and February 2016, U.A.E. CO employees (including Defendants) worked alongside and with numerous U.S. COMPANY ONE Raven Team employees (who were also U.S. persons) to provide cyber services for U.A.E. AGENCY ONE. During this time, U.S. COMPANY ONE repeatedly instructed its Raven Team employees that the TAA prohibited them from sharing ITAR-controlled information and details with U.A.E. CO employees. Despite those instructions, during this overlap period, U.A.E. CO managers, including Defendants, continued to access U.S. COMPANY ONE ITAR-controlled information, including information provided to U.A.E. AGENCY ONE under the TAA, to conduct CNE operations, without obtaining approval from the U.S. government or U.S. COMPANY ONE. In so doing Defendants and other U.A.E. CO CIO managers caused U.S. COMPANY ONE employees to discuss and reveal details about the Raven Team's TAA-governed cyber services to CIO personnel despite protests from U.S. COMPANY ONE employees who objected to providing such information to U.A.E. CO employees.

37. Throughout the Period, CIO, including the Defendants, expanded the breadth and increased the sophistication of the CNE operations that CIO was providing to the U.A.E. government.

38. As part of CIO's CNE operations throughout the Period, CIO employees whose activities were supervised by and/or known to the Defendants, obtained, without authorization

from the users or account providers, and used, again without authorization, targeted individuals' login credentials and other authentication tokens (*i.e.*, unique digital codes issued to authorized users) issued by U.S. companies, including providers of electronic and remote computing services such as email providers, cloud storage providers, and social media companies ("Providers"). With Defendants' knowledge or supervision, CIO employees then used these access devices and specially designed infrastructure to log into the target's accounts with the Providers to exfiltrate data back to CIO without the target's knowledge. Providers were unaware that Defendants used Providers' accounts, software, and computer hardware in connection with and furtherance of Defendants' CNE operations.

39. Throughout the Period, CIO employees whose activities were supervised by and/or known to the Defendants, carried out these CNE operations through the use of, among other things, anonymization services located in the United States and elsewhere, computer hacking tools bought in the United States and elsewhere, computer hardware that was bought in the United States, and e-mail, social media accounts, proxy servers, and computer hardware from U.S. companies. When obtaining email, social media, and server infrastructure accounts from U.S. companies throughout the Period, CIO employees, with the knowledge and supervision of Defendants, would obtain accounts ("Inauthentic Accounts") by providing fictitious or fraudulently-obtained user information. As part of their CNE operations during the Period, CIO employees, with the knowledge and supervision of Defendants, created hundreds of such Inauthentic Accounts with U.S. companies.

40. Throughout the Period, CIO employees, whose activities were supervised by and/or known to the Defendants, purchased and managed remote electronic infrastructure ("CIO Infrastructure") by obtaining anonymized servers on the Internet to avoid attribution. The CIO

Infrastructure was provisioned by CIO staff, and was used for all purposes, including target research, computer intrusion activities, and retrieval of exfiltrated data. CIO Infrastructure was located around the world and included accounts and servers that were obtained with fictitious or fraudulently-obtained identities as cover. Much of CIO Infrastructure was paid for through virtual currency, such as Bitcoin, that was circulated through "tumblers" to prevent anyone from connecting CIO to its infrastructure.

41. For example, throughout the Period, CIO CNE operations that Defendants supervised and/or knew about: (1) used Inauthentic Accounts, software, computers, and mobile devices issued by, obtained from, and maintained and supported by, U.S. COMPANY TWO to initiate and engage in CNE operations; (2) developed and sent code that was designed to provide unauthorized access to smartphones and other computers that used U.S. COMPANY TWO's services and software; (3) obtained and used, without authorization, login credentials and authentication tokens issued by U.S. COMPANY TWO; and, (4) obtained, through unauthorized access to accounts, servers, and computers in the United States and elsewhere operated by U.S. COMPANY TWO, information from internet-connected computers in the United States and elsewhere.

42. Similarly throughout the Period, CIO CNE operations that Defendants supervised and/or knew about: (1) used Inauthentic Accounts, software, computers, and mobile devices obtained from, and maintained and supported by, U.S. COMPANY THREE to initiate and engage in CNE operations; (2) developed and sent code that was designed to gain unauthorized access to smartphones and other computers that used U.S. COMPANY THREE services and software; (3) obtained and used, without authorization, login credentials and authentication tokens issued by U.S. COMPANY THREE; and (4) obtained, through unauthorized access to accounts, servers, and

computers in the United States and elsewhere operated by U.S. COMPANY THREE, information from internet-connected computers in the United States and elsewhere.

43. During the Period, Defendant BAIER and CIO purchased computer exploits from various U.S. companies for use in CIO's CNE operations.

44. Beginning in about February 2016, Defendants and CIO sought to develop, provide, and maintain a more sophisticated and productive CNE operation that could provide remote, unauthorized access to smartphones and mobile devices provided by U.S. COMPANY TWO. The services provided by U.S. COMPANY TWO included an electronic messaging service, referred to here as "MESSENGER." MESSENGER delivered text and multimedia messages across devices that connected to cellular or broadband internet networks, which transmitted signals using a range of radio frequencies. MESSENGER required participating devices to communicate with U.S. COMPANY TWO servers in the United States to send and receive messages. MESSENGER users' devices would communicate with U.S. COMPANY TWO servers in the United States even if both the sender and recipient(s) were located outside the United States. As detailed below, CIO, throughout the Period, with the support, direction, and/or supervision of each of the Defendants, used exploit code from two U.S. companies to create sophisticated CNE software suites that gave CIO the ability to access and obtain, without authorization, user data from mobile devices that used MESSENGER.

45. U.S. COMPANY FOUR developed EXPLOIT ONE, which could be delivered via MESSENGER, including through U.S. COMPANY TWO servers located in the United States, and provided "zero-click" remote access to smartphones and mobile devices using particular versions of U.S. COMPANY TWO's operating system. All smartphones and similar devices manufactured and sold by U.S. COMPANY TWO used this operating system. Zero-click exploits

provide unauthorized access to a computer system or device without any interaction by (or alerting of) the targeted user – that is, they require "zero clicks" by the target. CIO and Defendants became aware of EXPLOIT ONE in or about February 2016, and were interested in obtaining it for use in CIO's CNE operations. In or about April 2016, Defendants obtained authorization from U.A.E. CO to purchase EXPLOIT ONE from U.S. COMPANY FOUR and to modify it for CNE purposes.

46. In or about May 2016, BAIER, operating on behalf of U.A.E. CO and CIO, purchased EXPLOIT ONE from U.S. COMPANY FOUR. U.A.E. CO paid approximately $750,000 for EXPLOIT ONE by transferring funds from bank accounts outside the United States to the U.S. bank account of U.S. COMPANY FOUR.

47. As delivered to CIO by U.S. COMPANY FOUR, EXPLOIT ONE included features that limited its effectiveness as a computer hacking tool. First, U.S. COMPANY FOUR configured EXPLOIT ONE to trigger visible notifications to the user(s) of compromised devices. Second, although EXPLOIT ONE, once deployed, provided remote access to compromised devices, it did not independently collect information from compromised devices, and it did not cause compromised devices to perform any other actions that provided information about the device or its contents or user(s). Third, because EXPLOIT ONE did not have an anonymous delivery mechanism, targets or COMPANY TWO may have been able to trace any intrusion back to the sending party.

48. Defendants BAIER and ADAMS were in direct contact with U.S. COMPANY FOUR, and Defendant GERICKE worked directly on the project to integrate EXPLOIT ONE into an offensive system for use in CIO's CNE operations.

49. In order to effectively use EXPLOIT ONE for CNE Operations, CIO employees, with Defendants' support, direction, and/or supervision, modified EXPLOIT ONE and created an

integrated cyber exploitation system that: (1) combined the modified EXPLOIT ONE with other malicious software and malware that was developed or purchased by CIO (specifically, malware "agents" or "implants"); (2) created a graphic operator interface that they referred to as "Karmageddon;" (3) utilized a U.S. company's anonymization services and other proxy servers to prevent detection and mask the true origin of CIO intrusions; and, (4) created and used anonymized pathways for CIO employees to exfiltrate data and information, including authentication tokens, passwords, e-mails, and text communications, from the compromised devices. In so doing, CIO and Defendants created a zero-click computer hacking and intelligence gathering system specifically designed, developed, maintained and operated by CIO and allowed its users the capability to access tens of millions of devices that used COMPANY TWO's operating system for U.A.E. AGENCY TWO's intelligence purposes. Defendants and other CIO employees colloquially referred to this system, in its entirety, as "KARMA."

50. KARMA became less effective for CIO in about September 2016, after U.S. COMPANY TWO updated the operating system for its smartphones and other mobile devices. However, even after U.S. COMPANY TWO's 2016 update, the version of KARMA that integrated EXPLOIT ONE remained effective against COMPANY TWO devices that were not updated with the new version of its operating system.

51. U.S. COMPANY FIVE developed EXPLOIT TWO, which was, in effect, a more advanced version of EXPLOIT ONE. Like EXPLOIT ONE, EXPLOIT TWO was also delivered through MESSENGER, including through U.S. COMPANY TWO servers located in the United States. EXPLOIT TWO was also "zero-click" because it allowed remote access to targeted devices without any interaction by the device owner. The owner of U.S. COMPANY FIVE represented

to BAIER that, as delivered by U.S. COMPANY FIVE and prior to any subsequent modifications, EXPLOIT TWO was export designated as "EAR99."

52. Defendants BAIER and ADAMS were in direct contact with U.S. COMPANY FIVE during this period, and Defendant GERICKE worked directly on the project to integrate EXPLOIT TWO into an offensive system for CIO's CNE operations.

53. In or about October 2016, BAIER, operating on behalf of U.A.E. CO, purchased a package from U.S. COMPANY FIVE (the package included EXPLOIT TWO, other CNE tools, and maintenance services) for over $1,300,000. U.A.E. CO paid for EXPLOIT TWO by transferring funds from bank accounts outside the United States to the U.S. bank account of U.S. COMPANY FIVE.

54. As delivered by U.S. COMPANY FIVE to CIO, EXPLOIT TWO had features that limited its effectiveness as a computer hacking tool. Although EXPLOIT TWO, once deployed, provided remote access to compromised devices, it did not independently collect information from compromised devices, and it did not cause compromised devices to perform any other actions that provided information about the device, its contents or user(s). Additionally, because EXPLOIT TWO did not have an anonymous delivery mechanism, targets or COMPANY TWO may have been able to trace any intrusion back to the sending party if it was not modified prior to use by CIO.

55. EXPLOIT TWO was effective against U.S. COMPANY TWO's updated operating system and had several features that made it more useful for CIO's CNE operations than EXPLOIT ONE. For example, unlike EXPLOIT ONE, EXPLOIT TWO did not require the target device to be actively connected to Wi-Fi.

56. In order to effectively use EXPLOIT TWO for CNE Operations, CIO employees, with the Defendants' support, direction and/or supervision, modified EXPLOIT TWO and created an integrated cyber exploitation system that: (1) combined the modified EXPLOIT TWO with other malicious software (specifically, malware "agents" or "implants"); (2) created an efficient operator interface; (3) utilized a U.S. company's anonymization services and other proxy servers to prevent detection and mask the true origin of intrusions undertaken by CIO; and (4) created and used anonymized pathways for CIO employees to exfiltrate data and information, including access devices, authentication tokens, passwords, electronic mail and text communications, from the compromised devices. In so doing, CIO and Defendants created a powerful zero-click computer hacking and intelligence gathering system that was specifically designed, developed, maintained and operated by CIO and allowed its users the capability to access tens of millions of devices that used COMPANY TWO's operating system for U.A.E. AGENCY TWO's intelligence purposes. CIO employees colloquially referred to this system as "KARMA 2" or "KARMA, VERSION 2."

57. KARMA 2 was highly successful, and allowed CIO to compromise targeted devices in 90 to 95 percent of deployments. However, KARMA 2 became significantly less effective for CIO in or about August 2017, after COMPANY TWO again updated its software. However, even after August 2017, EXPLOIT TWO – and thus, KARMA 2 – remained effective against devices manufactured by COMPANY TWO that were not updated to the new version of its operating system.

58. Throughout the Period, Defendants BAIER and GERICKE and other U.S. person CIO employees working under Defendants' direction and supervision, purchased, designed, updated and maintained KARMA and KARMA 2 so that accessed devices automatically

transmitted authentication tokens, login credentials, and other data stored on the compromised devices to servers controlled by CIO.

59. Throughout the Period, CIO personnel, with Defendants' knowledge and direction, used authentication tokens and login credentials taken from KARMA and KARMA 2 attacks to gain unauthorized access to the corresponding accounts, systems, and servers, some of which were located in the United States.

60. During the Period, Defendants managed, led, and supported CIO employees who were responsible for thousands of offensive operations using KARMA and KARMA 2, and who thereby obtained information from devices accessed around the world.

61. On or about August 12, 2019, DDTC issued an opinion to the Federal Bureau of Investigation's liaison to DDTC that concluded that the services performed by CIO in connection with KARMA and KARMA 2 both constituted defense services under USML Category XI(d) because: (a) they were electronic intelligence gathering systems as described in USML Category XI(b); and (b) CIO assisted foreign persons in the use, design, development, engineering, production, modification, testing, maintenance, processing, or operation of KARMA and KARMA 2. DDTC further concluded that a license or other approval was required pursuant to the ITAR prior to providing any defense services in connection with KARMA and KARMA 2.

62. Throughout the Period, CIO employees whose activities were supervised by and/or known to the Defendants successfully conducted other CNE activities to gain access to computers around the world. These CNE activities targeted individual, corporate, and government targets by compromising computers and accounts belonging to associates, employees, or relatives of the primary targets. These activities included the following tactics and techniques:

a. "Spearphishing" campaigns implemented by sending fictitious messages, emails and documents containing malware embedded within a message or attachment;

b. Design, creation, customization, purchase, and use of other exploits and malware against computers connected to the internet that were used to take advantage of vulnerabilities in common software and operating systems created by U.S. companies; and

c. Use of password guessing programs to obtain access to protected computers, servers and hosting entities;

d. Design, creation, purchase, and use of computers and password guessing software purchased in the United States to access exfiltrated data that was encrypted.

**Defendants' Gains**

63. Between in or about January 2016 and December 2019, BAIER had gross gains of at least $750,000 from U.A.E. CO for the above activities, after subtracting amounts paid in U.S. federal income taxes over this period.

64. Between in or about January 2016 and December 2017, ADAMS had gross gains of at least $600,000 from U.A.E. CO for the above activities, after subtracting amounts paid in U.S. federal income taxes over this period.

65. Between in or about January 2016 and November 2018, GERICKE had gross gains of at least $335,000 from U.A.E. CO for the above activities, after subtracting amounts paid in U.S. federal income taxes over this period.

**Conclusion**

66. This proffer of evidence is not intended to constitute a complete statement of all facts known by the parties but is a minimum statement of facts intended to provide the necessary factual predicate related to the DPA. The limited purpose of this proffer is to demonstrate that

there exists a sufficient legal basis for the charged Information filed in conjunction with the DPA to proceed. This Factual Statement fairly and accurately summarizes and describes some of Defendants' actions and involvement in these offenses.

## DEFENDANT'S ACKNOWLEDGMENT

I have read this factual proffer and have discussed it with my attorney, Kenneth Wainstein, Esquire. I fully understand this factual proffer. I agree and acknowledge by my signature that this proffer of facts is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this factual proffer fully.

Date: 7 SEPTEMBER 2021

Marc Baier
Defendant

## ATTORNEY'S ACKNOWLEDGMENT

I have read this factual proffer, and have reviewed it with my client fully. I concur in my client's desire to adopt this factual proffer as true and accurate. To my knowledge, my client's decision to agree to and adopt this factual proffer is an informed and voluntary one.

Date: September 7, 2021

Kenneth Wainstein, Esq.
Counsel for the Defendant

DEFENDANT'S ACKNOWLEDGMENT

I have read this factual proffer and have discussed it with my attorney, Thomas G. Connolly, Esquire. I fully understand this factual proffer. I agree and acknowledge by my signature that this proffer of facts is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this factual proffer fully.

Date: 2021-09-07

Ryan Adams
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read this factual proffer, and have reviewed it with my client fully. I concur in my client's desire to adopt this factual proffer as true and accurate. To my knowledge, my client's decision to agree to and adopt this factual proffer is an informed and voluntary one.

Date: 2021-09-07

Thomas G. Connolly, Esq.
Counsel for the Defendant

## DEFENDANT'S ACKNOWLEDGMENT

I have read this factual proffer and have discussed it with my attorney, Michael S. Dry, Esquire. I fully understand this factual proffer. I agree and acknowledge by my signature that this proffer of facts is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this factual proffer fully.

Date: 9/7/2021

Daniel Gericke
Defendant

## ATTORNEY'S ACKNOWLEDGMENT

I have read this factual proffer, and have reviewed it with my client fully. I concur in my client's desire to adopt this factual proffer as true and accurate. To my knowledge, my client's decision to agree to and adopt this factual proffer is an informed and voluntary one.

Date: 9/7/2021

Michael S. Dry, Esq.
Counsel for the Defendant