

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 14-80031-CR-MARRA(s)(s)

UNITED STATES OF AMERICA

vs.

CHRISTOPHER R. GLENN,

Defendant.

_____ /

PLEA AGREEMENT

The United States Attorney's Office for the Southern District of Florida ("this Office") and **CHRISTOPHER R. GLENN** (hereinafter referred to as the "defendant") enter into the following agreement:

1. The defendant agrees to plead guilty to the following counts of the second superseding indictment: Count 1, which charges the defendant with unauthorized access, willful retention and failure to deliver national defense information, in violation of Title 18, United States Code, Section 793(e); Count 5, which charges the defendant with exceeding authorized access to a computer, obtaining national defense information and willfully retaining that information, in violation of Title 18, United States Code, Section 1030(a)(1); and Count 10, which charges the defendant with conspiracy to commit naturalization fraud, in violation of Title 18, United States Code, Sections 371 and 1425(a).

2. This Office agrees to seek dismissal of the remaining counts in the second superseding indictment, as to this defendant, after sentencing.

3. The defendant is aware that the sentence will be imposed by the Court after considering the advisory Federal Sentencing Guidelines and Policy Statements (hereinafter "Sentencing Guidelines"). The defendant acknowledges and understands that the Court will compute an advisory sentence under the Sentencing Guidelines and that the applicable guidelines will be determined by the Court relying in part on the results of a pre-sentence investigation by the Court's probation office, which investigation will commence after the guilty plea has been entered. The defendant is also aware that, under certain circumstances, the Court may depart from the advisory sentencing guideline range that it has computed, and may raise or lower that advisory sentence under the Sentencing Guidelines. The defendant is further aware and understands that the Court is required to consider the advisory guideline range determined under the Sentencing Guidelines, but is not bound to impose a sentence within that advisory range; the Court is permitted to tailor the ultimate sentence in light of other statutory concerns, and such sentence may be either more severe or less severe than the Sentencing Guidelines' advisory range. Knowing these facts, the defendant understands and acknowledges that the Court has the authority to impose any sentence within and up to the statutory maximum authorized by law for the offenses identified in paragraph 1 and that the defendant may not withdraw the plea solely as a result of the sentence imposed.

4. The defendant also understands and acknowledges that the Court may impose a statutory maximum term of imprisonment of up to 10 years, followed by a term of supervised release of up to 3 years. In addition to a term of imprisonment and supervised release, the Court may impose a fine of up to \$250,000.

RAD

AS TO COUNTS 1 AND 5 AND 5 YEARS' IMPRISONMENT

AS TO
COUNT 10,

(TR)
(CO)

5. The defendant further understand and acknowledges that, in addition to any sentence imposed under paragraph 4 of this agreement, a special assessment in the amount of \$300 will be imposed.

6. This Office agrees that it will recommend at sentencing that the Court reduce by two levels the sentencing guideline level applicable to the defendant's offense, pursuant to Section 3E1.1(a) of the Sentencing Guidelines, based upon the defendant's recognition and affirmative and timely acceptance of personal responsibility. If at the time of sentencing the defendant's offense level is determined to be 16 or greater, this Office will file a motion requesting an additional one level decrease pursuant to Section 3E1.1(b) of the Sentencing Guidelines, stating that the defendant has assisted authorities in the investigation or prosecution of the defendant's own misconduct by timely notifying authorities of the defendant's intention to enter a plea of guilty, thereby permitting the government to avoid preparing for trial and permitting the government and the Court to allocate their resources efficiently. This Office further agrees to recommend that the defendant be sentenced within the Sentencing Guidelines range, as that range is determined by the Court. This Office, however, will not be required to make this motion or this recommendation if the defendant: (1) fails or refuses to make a full, accurate and complete disclosure to the probation office of the circumstances surrounding the relevant offense conduct; (2) is found to have misrepresented facts to the government prior to entering into this plea agreement; or (3) commits any misconduct after entering into this plea agreement, including but not limited to committing a state or federal offense, violating any term of release, or making false statements or misrepresentations to any governmental entity or official.

7. The defendant is aware that the sentence has not yet been determined by the Court. The defendant also is aware that any estimate of the probable sentencing range or sentence that the defendant may receive, whether that estimate comes from the defendant's attorney, this Office, or the probation office, is a prediction, not a promise, and is not binding on this Office, the probation office or the Court. The defendant understands further that any recommendation that this Office makes to the Court as to sentencing, whether pursuant to this agreement or otherwise, is not binding on the Court and the Court may disregard the recommendation in its entirety. The defendant understands and acknowledges, as previously acknowledged in paragraph 3 above, that the defendant may not withdraw the plea based upon the Court's decision not to accept a sentencing recommendation made by the defendant, this Office, or a recommendation made jointly by the defendant and this Office.

8. The defendant is aware that Title 18, United States Code, Section 3742 and Title 28, United States Code, Section 1291 afford the defendant the right to appeal the sentence imposed in this case. Acknowledging this, in exchange for the undertakings made by the United States in this plea agreement, the defendant hereby waives all rights conferred by Sections 3742 and 1291 to appeal any sentence imposed, including any restitution order, or to appeal the manner in which the sentence was imposed, unless the sentence exceeds the maximum permitted by statute or is the result of an upward departure and/or an upward variance from the advisory guideline range that the Court establishes at sentencing. The defendant further understands that nothing in this agreement shall affect the government's right and/or duty to appeal as set forth in Title 18, United States Code, Section 3742(b) and Title 28, United States Code, Section 1291. However, if the United States appeals the defendant's sentence pursuant to Sections 3742(b) and 1291, the defendant shall

be released from the above waiver of appellate rights. By signing this agreement, the defendant acknowledges that the defendant has discussed the appeal waiver set forth in this agreement with the defendant's attorney.

9. The defendant knowingly and voluntarily agrees that the following property is subject to criminal forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1) upon conviction of the offense to which he agrees to plead guilty herein:

(a) Any personal property that was used or intended to be used to commit or to facilitate the commission of the violation to which he agrees to plead guilty herein; and

(b) Any property, real or personal, constituting or derived from, any proceeds that he obtained, directly or indirectly, as a result of the violation to which he agrees to plead guilty herein.

10. The defendant knowingly and voluntarily admits that the following personal property was used or intended to be used to commit the violation to which he agrees to plead guilty herein:

(a) One (1) Synology brand Network Attached Storage (NAS) device, model DS411 Slim, serial no. B8H9N00794, containing four 500 GB Western Digital hard drives with serial numbers: WX71E91JFPZ2, WX91A81W5290, WX41A6064475 and WX11E91EW171;

(b) One (1) Memorex 4x 4.7 GB DVD+RW disk marked "secret"; and

(e) One (1) Maxwell 16x 4.7 GB DVD-R disk labeled "PST Test 17-Feb-12", (collectively referred to hereinafter as the "Property").

11. The defendant knowingly and voluntarily agrees that upon the Court's acceptance

of his plea of guilty in accordance herewith, the Property shall be immediately forfeited to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A). Additionally, the defendant knowingly and voluntarily agrees that he shall not in any manner oppose the United States in seeking forfeiture of the Property.

12. The defendant knowingly and voluntarily agrees to waive his right to a hearing, pursuant to Fed. R. Crim. P. 32.2(b)(1)(A), to determine the requisite nexus between the Property and offense to which he agrees to plead guilty herein.

13. The defendant knowingly and voluntarily agrees to waive the following rights with respect to the forfeiture of the Property:

(a) All constitutional, legal, and equitable defenses to such forfeiture;

(b) Any constitutional or statutory double jeopardy defense or claim regarding such forfeiture; and

(c) Any claim or defense to such forfeiture brought or raised under the Eighth Amendment to the United States Constitution, including, but not limited to, any claim or defense of excessive fine.

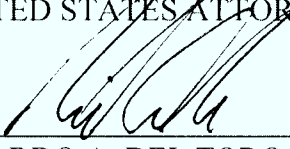
14. The defendant knowingly and voluntarily agrees and understands that forfeiture of the Property agreed upon herein shall not be treated as satisfaction (either partial or full) of any assessment, fine, restitution, cost of imprisonment, or any other penalty that the Court may impose upon the defendant in addition to the forfeiture.

15. This is the entire agreement and understanding between this Office and the defendant.

There are no other agreements, promises, representations, or understandings.


WIFREDO A. FERRER
UNITED STATES ATTORNEY

Date: 1-20-15

By: 

RICARDO A. DEL TORO
ASSISTANT UNITED STATES ATTORNEY

Date: 1/20/15

By: 

PATRICK MCKAMEY
ATTORNEY FOR DEFENDANT

Date: 1-20-15

By: 

CHRISTOPHER R. GLENN
DEFENDANT

FACTUAL PROFFER

United States v. Christopher R. Glenn
Case No. 14-80031-CR-MARRA(s)(s)

Counts 1 (Espionage) and 5 (Computer Intrusion)

1. **GLENN** is a United States citizen and was a civilian contractor working as a network system administrator for Harris Corporation stationed at the U.S. Army Southern Command's Joint Task Force Bravo (JTF-B), in Soto Cano Air Base, Honduras, between February and August 2012. Evidence collected in the investigation proves that **GLENN** took without authorization Department of Defense (DoD) classified documents and electronic messages (emails); then copied and transferred this classified information onto a computer hard drive; then copied the classified information onto a DVD disc that he took to his residence in Comayagua, Honduras; and then copied the classified files onto a Synology brand Network Attached Storage device and encrypted the files. **GLENN** also erased the computer event logs that tracked his actions. In addition to the unauthorized accessing, copying, converting, and stealing of classified materials, **GLENN** executed on the unclassified computer system of JTF-B a wiretapping program and two password revealing programs. This wiretapping program can be used for legitimate system administrator functions but also to steal network data in transit including passwords and other sensitive information.

2. **GLENN** was hired by Harris Corporation around February 2012 to work as an information technology (IT) contractor in the role of system administrator at JTF-B in Soto Cano Air Base, and tasked to implement the Windows 7 operating system on the JTF-B unclassified and classified systems as well as other system administrator functions.

3. Classified information is defined by Executive Order No. 13526, 75 Fed. Reg. 707

(January 5, 2010), as information in any form that (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories of information set forth in the order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Under the executive order, the designation "SECRET" is applied to information, the unauthorized disclosure of which, could reasonably be expected to cause serious damage to the national security.

4. Pursuant to the executive order, classified information can generally only be disclosed to those persons who have been granted an appropriate level United States government security clearance **and** possess a need to know the classified information in connection to their official duties. As a computer network system administrator and contractor for Harris Corporation at JTF-B at Soto Cano Air Base, **GLENN** held a SECRET security clearance. As a condition of his security clearance, **GLENN** had signed classified information nondisclosure agreements with the United States, acknowledging that "unauthorized retention of classified information . . . could cause damage or irreparable injury to the United States or could be used to the advantage of a foreign nation." Defendant **GLENN** also acknowledged and agreed in these nondisclosure agreements that he "shall return all classified materials which have, or may come into my possession . . . upon the conclusion of my employment or relationship with the Department or Agency that . . . provided me access to classified information."

5. On or about Sunday, June 17, 2012, **GLENN** went to the JTF-B Network Operations Center (NOC), a secure work area where the computer system administrators worked. A forensic examination of a computer hard drive that **GLENN** used at a classified computer terminal at the NOC revealed that on Sunday, June 17, 2012, **GLENN** used his individually-assigned JTF-B computer account to sign onto a JTF-B Secure Internet Protocol Router (SIPR)

computer terminal and create a folder on the SIPR hard drive labeled "DOCS". The DOCS folder contained three sub-folders, which contained 18 files, which were created or copied into the folder by **GLENN** on or about June 17, 2012. Seventeen of these 18 files contained information classified up to the SECRET level which **GLENN** took and converted from the SIPR email account of another individual who was then the JTF-B Commander. These 17 files were either email messages or email message file attachments and documents which originated from the JTF-B Commander's SIPR email Inbox folder. The 18th file that **GLENN** copied onto the DOCS folder consisted of the contents of the JTF-B Commander's entire SIPR email account called the Microsoft Outlook Personal Storage Table (PST), which contained over 1,000 emails, many of which were classified up to the SECRET level. The JTF-B Commander has confirmed that he never authorized **GLENN** to take or copy either his entire SIPR email account or any email or document within it. Therefore, **GLENN** did not have the authority to possess, access or control the JTF-B Commander's SIPR PST email account or any emails or documents contained therein.

6. The forensic examination of the SIPR hard drive that **GLENN** used on June 17, 2012, further revealed that several minutes after creating the DOCS folder on his classified hard drive, **GLENN** unsuccessfully attempted to burn (create) a DVD disk and received an error message from the disk burning software indicating that his access was denied because the SIPR computer terminal he was using was not authorized to copy or burn classified materials onto removable media such as a DVD. In fact, only two individuals at JTF-B were authorized to do so and had computers that were authorized to copy classified materials onto removable media. **GLENN** was not one of them. After the first unsuccessful attempt to burn a DVD, **GLENN** successfully initiated the burning of a DVD disk whose volume label was "DOCS" and contained three folders and 18 files. **GLENN** successfully completed this process a few minutes

after the first attempt. In order to successfully create the DVD disk containing the classified materials, **GLENN** had to disable and override system security protections which had first prevented him from creating the DVD. **GLENN** then copied the three subfolders and 18 files belonging to the JTF-B Commander, including the classified files and entire SIPR PST account onto the DVD that **GLENN** burned.

7. Forensic analysis has confirmed that the 18 files that **GLENN** copied onto the DVD disk were the same files that **GLENN** first copied onto the DOCS folder in the SIPR computer terminal's hard drive that **GLENN** used on June 17, 2012, at the JTF-B NOC.

8. Immediately after burning the classified files onto a DVD, **GLENN** cleared the Windows event log files, meaning that he tried to delete from the computer system evidence of the steps that he took to copy the JTF-B Commander's classified files and the steps that he took to transfer them onto a DVD.

9. On or about August 27, 2012, Army investigators and JTF-B personnel seized hard drives from both the SIPR (classified) network computers and the unclassified network computers and associated removable media such as CD/DVD disks, and hard drives in and around **GLENN**'s JTF-B work space as potential evidence for examination. One of the hard drives seized on this day was the classified (SIPR) hard drive that **GLENN** had used on or about June 17, 2012, to copy the then JTF-B Commander's classified email messages and documents. However, the DVD that **GLENN** burned on or about June 17, 2012, containing the JTF-B Commander's classified documents and emails was not found in **GLENN**'s work space and was not located by Army investigators who searched it. In October 2012, **GLENN**'s employment with Harris Corporation at JTF-B was terminated.

10. On or about March 11, 2014, Honduran police obtained a judicially authorized warrant to search a house that **GLENN** maintained in Comayagua, Honduras, near Soto Cano

Air Base, in order to search for evidence of unrelated suspected crimes. The Honduran police search of **GLENN**'s residence in Honduras revealed that he maintained computers, servers, removable media, and other electronic equipment including one Synology brand Network Attached Storage device. Among the removable media seized by Honduran police were numerous DVDs. One of the DVDs seized by Honduran police contained all of the same classified files that **GLENN** burned onto a DVD on June 17, 2012, including the entire classified email account of the former JTF-B Commander and the classified documents contained in the email account. The Synology Network Attached Storage device also contained all of the same classified documents and emails in an encrypted electronic folder. **GLENN** never returned the classified files that he had copied onto the SIPR computer hard drive, onto the DVD that he burned on June 17, 2012, or onto the Synology Network Attached Storage device to any person entitled to receive those classified files. Neither **GLENN**'s residence nor the Synology Network Attached Storage device were authorized or certified by U.S. government officials to store classified materials.

11. The classified emails and documents, as described in Counts 1 and 5 of the Second Superseding Indictment, which **GLENN** copied onto his account in the classified (SIPR) computer terminal at JTF-B and which **GLENN** burned onto a DVD on June 17, 2012, and which **GLENN** encrypted and copied onto the Synology Network Attached Storage device found in his residence in Honduras all constitute national defense information because they relate to the national defense and **GLENN** had reason to believe that they could be used to the injury of the United States or to the advantage of any foreign nation. After copying the national defense information onto his SIPR account, onto a DVD and onto the Synology Network Attached Storage device found in **GLENN**'s Honduran residence, **GLENN** willfully retained and failed to deliver the national defense information to any officer or employee entitled to receive it.

Count 10 (Conspiracy to Commit Naturalization Fraud)

12. Starting on or about April 20, 2007, **GLENN** and his purported second wife, **KHADRAA A. GLENN (KHADRAA)** conspired to obtain naturalization for **KHADRAA** through a pattern of material false statements, fabrication and submission of materially fraudulent documents and fraud perpetrated against U.S. Citizenship and Immigration Services (USCIS). On or about April 20, 2007, **GLENN** submitted to USCIS a Relative Immigrant Visa Petition Form I-130 on behalf of **KHADRAA** stating that he had divorced his first wife, "M.T.A.," on December 20, 2006, and that **GLENN** and **KHADRAA** had been married on March 23, 2007. The Form I-130 sought an immigrant visa on behalf of **KHADRAA**, claiming her as **GLENN**'s spouse, which was the first step toward the eventual naturalization of **KHADRAA**.

13. **KHADRAA** and **GLENN** subsequently submitted to USCIS a divorce decree indicating that **GLENN** had divorced "M.T.A." on April 22, 2007, not on December 20, 2006, which was two days after the date on which **GLENN** submitted the Form I-130 claiming that he was already married to **KHADRAA**. **KHADRAA** and **GLENN** also submitted to USCIS a marriage certificate dated April 23, 2007, which also directly contradicted the statement on the Form I-130 claiming that the purported marriage between **GLENN** and **KHADRAA** had taken place on March 23, 2007.

14. On or about January 16, 2008, in response to a demand from USCIS for proof that his purported divorce from "M.T.A." in Jordan was legally valid in order to establish the legality of his subsequent marriage, **GLENN** sent an e-mail message to several e-mail addresses requesting: "I just need a rental lease for an apartment in Amman, Jordan. It should be blank (empty) and in Arabic. I will translate it to English, but it is so urgent please help me."

15. On or about January 16, 2008, **GLENN** sent an e-mail message to KHADRAA requesting: "Please email alit1954@yahoo.com and ask him to get me a blank (empty) 1 page basic rental agreement (lease) from Amman, Jordan in Arabic. His name is Ali, and works for Barih company. He doesn't write or read English, so I need your help to create the email. Please CC me so I can ask Ziad and everyone else I know later with your email."

16. On or about January 16, 2008, KHADRAA replied to an e-mail message from **GLENN** stating: "See the Arabic writing below:-) hope that helps:-) basically I am requesting his help to write a rental agreement or if he has one he can send it to me by email through scan it."

17. On or about January 16, 2008, **GLENN** received an e-mail message with an attachment entitled "rental agreement lease.doc" from an individual using the email address ziad@ziadcom.com.

18. On or about January 16, 2008, **GLENN** sent an e-mail message to KHADRAA asking: "Is this good? Can you can you change it to Amman, Jordan?..."

19. On or about January 16, 2008, KHADRAA replied to an e-mail message from **GLENN** stating: "It is great, is the rules in the rent agreement Egyptian or Jordanian? If it is Egyptian then we can only use the first page because the rest of the pages stating Egyptian rules but not Jordanian."

20. On or about February 2, 2008, KHADRAA sent an e-mail message to **GLENN** with an attachment entitled "3 – Exhibit A – Rental Agreement Lease.doc".

21. On or about February 2, 2008, KHADRAA sent an e-mail message to **GLENN** with a subject line stating: "FW: 3 rent Agreement (UNCLASSIFIED)", with an attachment entitled "Document.pdf", which contained two signed Jordanian lease agreements, each with a

corresponding English translation purporting to show that **GLENN** had leased an apartment in Amman, Jordan, from October 2005 until April 26, 2007.

22. On or about February 2, 2008, in response to a USCIS request for proof that he resided in Jordan at the time of his purported Jordanian divorce, **GLENN** sent a letter dated February 1, 2008, to USCIS claiming that he had leased an apartment in Amman, Jordan, from October 2005 to April 26, 2007, and attaching as "Exhibit A" the same two Jordanian lease agreements, each with a corresponding English translation which KHADRAA had sent to **GLENN** in a February 2, 2008, email message that had an attachment entitled "Document.pdf".

23. On or about December 10, 2009, KHADRAA signed an Application for Naturalization Form N-400, attaching a purported Jordanian divorce decree dated April 22, 2007, to attempt to prove that **GLENN** had legally divorced his first wife, "M.T.A.," on April 22, 2007.

24. In an April 2010 Google chat, **GLENN** coached KHADRAA to lie in her naturalization interview with USCIS by telling the interviewer that she resided in Honduras with **GLENN**, when in truth, she resided in Australia at the time. **GLENN** further coached KHADRAA to buy a one-way ticket to Honduras to deceive the USCIS interviewer into thinking that KHADRAA lived in Honduras with **GLENN**.

25. In a June 2010 Google chat, **GLENN** again coached KHADRAA to lie in her naturalization interview with USCIS by telling the interviewer that she did not work or reside in Australia, when in truth, KHADRAA did reside and work in Australia at the time. In a letter dated October 18, 2013, in support of KHADRAA's appeal of the denial of her security clearance, **GLENN** admitted that KHADRAA remained working for an Australian government agency in Australia for two years after February 2010, while **GLENN** worked in Honduras.

26. On June 29, 2010, KHADRAA completed her naturalization interview and on July 20, 2010, KHADRAA obtained U.S. citizenship through naturalization.

I hereby affirm that the factual proffer above is true and correct.

Date: 1/23/15

By: 
CHRISTOPHER R. GLENN
DEFENDANT