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.
_____/

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENSE OBJECTIONS TO THE PRE-SENTENCE INVESTIGATION REPORT AND SENTENCING POSITION MEMORANDUM

The United States hereby files the Government's Sentencing Position Memorandum and Response in Opposition to the Defendant's Objections to the Pre-Sentence Investigation Report. For the reasons discussed below, this Court should deny Defendant CHRISTOPHER R. GLENN's (GLENN's) objections and sentence him to the statutorily authorized maximum sentence of 120 months as to Counts 1 and 5 to run concurrently to each other, and 12 months of imprisonment as to Count 10, to run consecutively to Counts 1 and 5, which is a combined sentence that is lower than the advisory guideline imprisonment range.

A. Background and Relevant Conduct

GLENN pled guilty to Count 1, unauthorized access, willful retention and failure to deliver national defense information (NDI), in violation of 18 U.S.C. § 793(e); Count 5, exceeding authorized access to a computer and thereby obtaining and willfully retaining national defense information, in violation of 18 U.S.C. § 1030(a)(1); and Count 10, conspiracy to commit naturalization fraud, in violation of 18 U.S.C. §§ 371 and 1425(a). During his change of plea hearing, GLENN admitted his criminal conduct, as detailed in the Government's factual proffer,

which is incorporated into the Pre-Sentence Investigation Report's (PSI) Offense Conduct. PSI (DE:107) at ¶¶ 5-20 and 23-35; (DE:101 at 8-16).

Computer Intrusion & Theft of Classified Materials

On Sunday, June 17, 2012, GLENN, a computer system administrator at the Joint Task Force-Bravo (JTF-B) Network Operations Center (NOC) located at the Soto Cano Air Base in Honduras, used his individually-assigned JTF-B computer account to sign onto the JTF-B Secret Internet Protocol Router (SIPR) computer system[1] to steal classified emails, intelligence reports and military plans belonging to the JTF-B Commander. GLENN created a folder labeled "DOCS" on the SIPR (classified) computer terminal he was working on. This folder contained 18 files belonging to the JTF-B Commander that GLENN selected and placed in three sub-folders. *See* Exhibit 1, Screenshots of the DOCS folder on the SIPR computer.[2] Seventeen of these 18 files were either email messages or email message file attachments 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, with over 1,000 emails, many of which were classified at the SECRET level. The JTF-B Commander confirmed that he never authorized GLENN or anyone else to take or copy either his entire SIPR email account or any document within it.

[1] The SIPR computer system is a classified computer system used to perform word processing, email communication and other computer functions in a secure computer network that processes documents and information classified up to the SECRET level.

[2] The exhibits and attachments to this memorandum [Exhibits 1-22] have not been filed in the public docket because they contain sensitive national security information, personal identifying information about certain individuals or classified information. They are also covered by this Court's Protective Order. [DE:29]. Accordingly, those exhibits have been provided to the Court and to the defense separately.

A forensic examination revealed that several minutes after creating the folder containing the stolen classified materials on his hard drive, GLENN unsuccessfully attempted to burn (create) a DVD disk, but received an error message indicating that his access was denied because the SIPR computer terminal was not authorized to copy or burn classified materials onto removable media like DVDs. After the first unsuccessful attempt, GLENN disabled and overrode system security protections which had first prevented him from creating the DVD and successfully burned the DVD disk containing the same 18 files in three sub-folders including the JTF-B Commander's entire SIPR email account. *See* Exhibit 2, Screenshots of the DOCS folder on the DVD. Immediately after burning the stolen classified files onto the DVD, GLENN cleared the Windows security 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. *See* Exhibit 3, Forensic Timeline of the SIPR Hard Drive.

On or about March 11, 2014, Honduran police obtained a warrant to search a house where GLENN resided in Comayagua, Honduras, near the base. The Honduran police searched GLENN's residence and seized computer equipment and removable digital media. Among the removable media seized by Honduran police was a DVD containing the same 18 files including the JTF-B Commander's entire classified email account that GLENN stole on June 17, 2012. *See* Exhibit 2. Also among the electronic equipment seized from GLENN's residence was a Synology brand computer storage device (the Synology device), which stored a hidden and encrypted compartment labeled "2012 Middle East" into which GLENN had again copied the same three sub-folders and 18 files, including the JTF-B Commander's entire classified email account that GLENN stole on June 17, 2012. *See* Exhibit 4, Screenshots of the 2012 Middle

East compartment on the Synology Device. The encryption software that GLENN used to conceal the stolen classified materials in the Synology device is a program called TrueCrypt. In October 2011, GLENN had sent an email to an associate with an internet hyperlink to an article entitled "FBI hackers fail to crack TrueCrypt." Exhibit 5, Email Dated October 14, 2011. In this case, the FBI did decrypt GLENN's hidden files containing the stolen classified materials.

GLENN's Attempt to Tamper With Evidence

On February 28, 2014, while in pre-trial detention at the Palm Beach County Jail, GLENN made a recorded telephone call to his mother. In the call, GLENN told her to send a message to his associate to "tell Sinia. . . to disconnect. . . the black box. . . with the blinking lights. . . on top of the batteries." *See* Exhibit 6, Transcript of Jail Call at 2-3; Exhibit 7, Picture of Synology Black Box on Top of Batteries. Sinia is an 18 year old girl who was living with GLENN at his house in Honduras. The "black box" was the Synology device found by Honduran police at GLENN's compound containing the encrypted compartment that stored the classified materials that GLENN stole on June 17, 2012. The reason GLENN tried to send a message to Sinia to disconnect the black box is because he wanted to prevent law enforcement from discovering what the Synology contained. *See* Exhibit 6, Transcript of Jail Call at 2 ("I've got some pictures of me and Kadra [sic] that are private and I think they are gonna look through um [sic]. . . .").

GLENN's False Statements to the Government

The case agents and prosecutors met with GLENN and his counsel on January 20, 2015, to determine what GLENN did with the stolen classified materials. GLENN gave false answers to numerous questions about why and how he stole the classified materials, and what he did with it after stealing it. *See* Exhibit 8, FBI 302 Report of Interview. For example, GLENN stated

that he only burned the DVD containing the classified materials to be proactive in case someone asked for it; and that he put the disc in his desk drawer; and mistakenly took the disc out of a secure building in the base; and mistakenly took the disc to his house; and again mistakenly copied the stolen classified materials from the disc into an encrypted compartment within his Synology computer storage device. *Id*. at 2-3. GLENN claimed that he was not even aware of what he had done, and had never again accessed the classified files that he had "mistakenly" copied onto his Synology device. *Id*. at 3. GLENN also claimed that he erased all the security log files on the SIPR computer terminal *while* copying the DVD disc containing the classified materials because the SIPR computer froze while GLENN was working on it. *Id*. at 2.

The forensic analysis proves that GLENN's statements are false. First, the forensic analysis of the classified/SIPR computer showed that the computer did not freeze but rather that GLENN deleted the security log files *after* he successfully copied all the Commander's emails and documents onto the DVD disc, evincing his intent to conceal the computer intrusion. Second, GLENN first selected 17 individual military intelligence reports and other classified documents that he segregated into three sub-folders on his SIPR account, an act that proves his intent was to surreptitiously steal classified materials, not create a back-up of a complete email account. Third, forensic analysis has also determined that GLENN deliberately (not mistakenly) copied the stolen classified materials into an encrypted-hidden compartment on the Synology computer storage device at his residence.

Naturalization Fraud

GLENN also pled guilty to conspiracy to fraudulently obtain naturalization for his purported wife, KHADRAA GLENN (KHADRAA) through a pattern of false statements, fabrication and submission of fraudulent documents to United States Citizenship and Immigration

Service (USCIS). PSI (DE:107) at ¶¶ 23-35; (DE:101 at 13-16). Their fraudulent scheme eventually led to KHADRAA's naturalization.

B. GLENN's Objections to the PSI

GLENN has objected to numerous paragraphs of the PSI in which he contradicts the admissions he made in his factual proffer and which are inconsistent with the evidence provided to him in discovery. The Government addresses only those objections which have any bearing on the Court's guidelines calculation or sentencing factors pursuant to 18 U.S.C. § 3553(a).

GLENN objects to paragraphs 11-12, claiming that he "never misled JTF-B technicians as to his true unclassified hard drive." (DE:128 at 2). These paragraphs do not affect the guidelines calculations. However, GLENN did mislead the technicians when he provided two false hard drives on the first incident when the technicians tried to seize GLENN's unclassified hard drive. When the technicians returned a second time to seize GLENN's true hard drive involved in the malware incidents, GLENN tried to tamper with his hard drive and had to be physically restrained by a supervisor so that technicians could seize the hard drive. *See* Exhibit 9, Interview Report of K.F.E. The reason GLENN misled JTF-B technicians is because he had stolen the unclassified emails of other JTF-B members and those were later found by forensic analysis on GLENN's unclassified hard drive.

GLENN objects to paragraph 14 of the PSI, which is essentially his offense conduct taken nearly verbatim from paragraph 5 of his signed factual proffer, and which GLENN acknowledged was true at his change of plea hearing. (DE:101 at 9-10). This Court can rely on the factual proffer in making sentencing findings. *See United States v. Day*, 943 F.2d 1306 (11th Cir. 1991) (district court properly used stipulated facts in the plea agreement to calculate the base offense level). The crux of GLENN's objection is that he was tasked with transferring

the Blackberry contacts list from the previous to the new JTF-B commander and that, based on that task, he decided to then copy the commander's entire unclassified email account and entire classified (SIPR) account to be "proactive." This objection and GLENN's factual allegations are false and completely contrary to the evidence including his signed factual proffer.

First, GLENN cannot explain how transferring an unclassified contacts list on a mobile phone has anything to do with stealing 17 individual classified intelligence reports and messages, and the entire classified email account of the commander. His claim is illogical and contrary to the evidence and common sense. How does a request to back up a contacts list on a mobile phone morph into a scheme to hack into the commander's classified email account, disabling computer system security protections, unauthorized copying of classified materials onto discs, erasing the security log files to conceal his crimes, taking the disc containing the stolen classified materials to his home and then copying the classified materials onto an encrypted-hidden compartment in his home computer storage device?

Second, GLENN selectively picked 17 individual classified intelligence reports and messages relating to the Middle East and the Persian Gulf region from the commander's SECRET account and placed them in three sub-folders in the SIPR computer terminal. *Id*. at 10 (¶5); Exhibit 1, Screenshots of the DOCS folder on the SIPR computer. GLENN was not creating a back-up for the Commander's email account in case he asked for them. GLENN was inspecting and copying individual files that he found of interest and segregating them into separate sub-folders in GLENN's own personal SIPR account. *Id*. This methodical mining of classified information proves beyond any doubt, that GLENN's crime was a premeditated computer intrusion and hacking that later led him to copy the entire classified email account into

two additional unauthorized digital storage media that were eventually recovered from GLENN's personal residence nearly two years later.

GLENN's objection to paragraph 14 of the PSI is therefore completely inconsistent with paragraphs 5, 6, 8, 10, and 11 of his signed factual proffer [DE:101 at 8-16], where he admitted the exact conduct that he now contests in his objection. In fact, GLENN now even denies that he intended to "steal or convert" the JTF-B commander's classified materials and instead claims that his conduct was only "negligent and reckless." (DE:128 at 4). This denial conflicts with GLENN's admission in his signed factual proffer that his conduct constituted "unauthorized accessing, copying, **converting**, and **stealing** of classified materials." [Emphasis added] (DE:101 at 8 (¶1)). GLENN's self-contradictory objection undermines his claim of acceptance of responsibility. (DE:128 at 12). GLENN's objection to paragraph 14 of the PSI should be denied because the forensic evidence and GLENN's own factual proffer refute his allegations.

GLENN also objects to paragraph 15 of the PSI and now claims that he was not aware that he lacked authority to disable the computer security protections and to then burn classified materials onto removable media such as a DVD. (DE:128 at 4). GLENN's signed factual proffer plainly contradicts this objection. In the proffer, GLENN admitted that he "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***." [Emphasis added]. (DE:101 at 10 (¶6)). Four other JTF-B system administrators

and personnel have also confirmed this fact. *See* Exhibit 22. Based on his own admission and the evidence, GLENN's objection to paragraph 15 should be denied.

GLENN also objects to paragraph 16 of the PSI and now alleges that he did not delete the Windows event log files to conceal evidence of the steps he took to copy the JTF-B Commander's classified files, but rather that he did so ***before*** burning the classified files because the computer was running slowly. (DE:128 at 5). GLENN's signed factual proffer clearly contradicts this objection. In the signed proffer, GLENN admitted that "[i]mmediately ***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." [Emphasis added]. (DE:101 at 11 (¶8)). The forensic analysis of the SIPR computer's hard drive also confirms the factual proffer. It shows that GLENN successfully copied the classified materials onto a DVD at 1:55 p.m., but only deleted the Windows event log files ***after*** he had burned the stolen classified files onto a DVD at 1:59 p.m., and then immediately shut down the computer at 2:00 p.m. *See* Exhibit 3, Forensic Timeline of the SIPR Hard Drive.

GLENN objects to paragraph 18 of the PSI. (DE:128 at 6). It is unclear what GLENN objects to in light of his admission that he was draining his bank accounts after being suspended for the malware incidents. In any case, this objection does not affect the calculation of the guidelines.

GLENN objects to paragraph 20 of the PSI, and now claims that although he allowed two foreign nationals, A.A. and Y.A.E., to remotely access the Synology storage device that contained the stolen classified materials, they never actually connected to it, and that he never transferred any classified information to these two individuals or any other party. *Id.* This

objection is inconsistent with GLENN's admission during his debriefing with the government, when he admitted that both foreign nationals connected to and accessed various files on the Synology device. *See* Exhibit 8, FBI 302 Report of Interview at 3. The objection should be denied.

GLENN also objects to paragraphs 21-22, detailing his misconduct as an independent contractor in Forward Operating Base (FOB) Bucca, Iraq. (DE:128 at 6-9). GLENN denies that he ever defrauded the government of goods and services, gained unauthorized access to government databases, or engaged in any fraud or computer hacking. *Id*.

Between March 2008 and January 2009, GLENN engaged in an extensive pattern of criminal misconduct including fraud, theft of government goods and services, and computer hacking while working as an independent contractor for two Iraqi companies in FOB Bucca, Iraq. *See* Exhibit 10, Investigation Report of U.S. Army Criminal Investigations Division (CID). The CID investigation revealed that GLENN gained access to military computer databases to create unauthorized access badges for Iraqi workers that allowed them unescorted access to the U.S. military base. *Id*. at 9-10; PSI at ¶ 21. GLENN had also created false documents and Common Access Cards (CACs), which are federal civilian employee identifications, and falsely impersonated a GS-15 federal employee, to gain unauthorized access to government goods and services. *See* Exhibit 10 at 9-10; PSI at ¶¶ 21-22. GLENN admitted to an Army investigator that he falsified a memorandum claiming to be a postal officer. Exhibit 10 at 3. GLENN hacked and collected digital information from numerous individuals at FOB Bucca. PSI at ¶ 22; *See* Exhibit 11 at 7-8, 12, CID Interviews of M.T.A. and J.W.B. Based on the Army CID investigation, the Base Commander made a finding that there were "reasonable grounds to believe that [GLENN had] individually and collectively with [KHADRAA]

committed serious frauds upon the U.S. Government. . . Under false pretenses, [GLENN] obtained a fraudulent Common Access Card (CAC), obtained unauthorized services, and improperly gained access to government computer systems." Exhibit 12, Expulsion Letter. Although GLENN was not prosecuted for the approximately $17,000 worth of fraud he committed, the Base Commander made an administrative finding of misconduct based on violations of the Uniform Code of Military Justice and under federal law, and permanently expelled and barred GLENN from the base. *Id*. GLENN did not appeal the Base Commander's findings.

The numerous witnesses and evidence cited in the CID Report prove GLENN's misconduct by a preponderance of the evidence. *Cf. United States v. Faust*, 456 F.3d 1342, 1347 (11th Cir. 2006) (acquitted conduct can be considered relevant conduct if proved by a preponderance of the evidence); *United States v. Rivera-Lopez*, 928 F.2d 372-73 (11th Cir. 1991). GLENN's objection to paragraphs 21-22 should therefore be denied.

GLENN also objects to paragraphs 38 through 40 and 48 of the PSI which accord him a two point enhancement pursuant to U.S.S.G. § 3C1.1[3] for attempting to obstruct justice by providing false statements to the Government during his debriefing, attempting to tamper with evidence -- the Synology device -- and plotting an escape attempt from the Palm Beach County Jail during pre-trial detention. (DE:128 at 9-10, 12). GLENN's objection should be denied. GLENN gave numerous false statements during his debriefing. *See* Exhibit 8, FBI 302 Report of Interview. For example, GLENN stated that the reason that he burned a DVD containing the

[3] Guidelines Section 3C1.3 states in relevant part: "If (1) the defendant willfully. . . attempted to obstruct or impede, the administration of justice with respect to the investigation, prosecution, or sentencing of the instant offense of conviction and (2) the obstructive conduct related to (A) the defendant's offense of conviction and any relevant conduct, . . . increase the offense level by **2** levels."

commander's classified materials was to be proactive in case someone asked for it; and that he put the classified DVD in his desk drawer; and mistakenly took the classified DVD out of a secure building from the base; and mistakenly took the classified DVD to his house, and he again mistakenly copied the stolen classified emails and documents from the DVD to a hidden and encrypted folder in his Synology storage device. *Id*. at 2-3. GLENN claimed that he was not even aware of what he had done, but contradicted himself during the debriefing by admitting that he had opened some of the stolen classified emails because he noticed they were about the Middle-East. *Id*. at 2. GLENN also claimed that he erased all the security log files on the classified (SIPR) computer terminal ***while*** copying the DVD containing the JTF-B Commander's classified email account because the SIPR computer froze while GLENN was working on it. *Id*. at 2. This statement is inconsistent with GLENN's suggestion in his objection to paragraph 16 of the PSI that he erased the log files ***before*** copying the classified files because the computer was running slowly. (DE:128 at 5). In any case, both claims are false.

GLENN's debriefing statements defy logic and common sense and are inconsistent with GLENN's signed factual proffer and with the forensic evidence. First, the forensic analysis of the SIPR computer established that it did not freeze but rather that GLENN deleted the security log files ***after*** he successfully copied all the classified emails and documents onto the DVD disc, evincing his intent to conceal the computer intrusion. *See* Exhibit 3, Forensic Timeline of the SIPR Hard Drive. Second, GLENN disabled the classified computer's security system's prohibition on copying classified materials onto a disc in order to burn the DVD. Third, forensic analysis has also determined that GLENN did not mistakenly copy the stolen classified materials into the Synology computer storage device, but instead deliberately secreted them into a hidden-encrypted compartment. *See* Exhibit 4, Screenshots of the "2012 Middle East"

compartment on the Synology Device. Forensic analysis of the Synology device thus showed that GLENN went to great lengths to conceal the stolen classified materials by putting them in a hidden container and further encrypting them to make them inaccessible to law enforcement. In fact, GLENN's intent to conceal his hacking and theft of military secrets from the FBI is evident in an email he sent to his associate containing an article suggesting that the FBI could not crack TrueCrypt, the very software GLENN used to encrypt the stolen classified materials onto the Synology device. *See* Exhibit 5, Email Dated October 14, 2011.

GLENN's false statements to prosecutors and investigators at his debriefing were purposely made to impede and mislead the investigation. Because he lied about his crimes, the Government is unable to rely on his claim that he did not transfer the classified materials to an unauthorized person or foreign power. Nor can the Government assess the potential damage that GLENN caused with his theft of national defense information. GLENN's false and misleading statements about his computer intrusion and theft of classified materials constitute exactly the type of misconduct that the Eleventh Circuit has found to qualify for an obstruction of justice enhancement pursuant to U.S.S.G. §3C1.1. *See United States v. Uscinski*, 369 F.3d 1243, 1247 (11th Cir. 2004) (defendant concocted a false, exculpatory story that caused law enforcement to further investigate the crime); *United States v. Salemi*, 26 F.3d 1084, 1087 (11th Cir. 1994) (defendant's false statement to police that he did not know his wife's whereabouts impeded and misdirected the police efforts to find the victim kidnapped by defendant's wife). Like the defendants in *Salemi* and *Uscinski*, GLENN made false statements to investigators that misdirected Government efforts to determine what happened to the stolen classified materials and whether GLENN gave access to these materials to an unauthorized person or foreign power.

The second basis of the obstruction enhancement is GLENN's attempt to tamper with the Synology device. GLENN's intent to obstruct justice was evident from his own recorded words. In the recorded telephone call GLENN sent a message to his associate to "tell Sinia. . . to disconnect. . . the black box. . . with the blinking lights. . . on top of the batteries." *See* Exhibit 6, Transcript of Jail Call at 2-3; Exhibit 7, Picture of Synology Black Box on Top of Batteries. The "black box" was the Synology device. The reason GLENN tried to send a message to Sinia to disconnect the black box is because he wanted to prevent law enforcement from discovering what the Synology device contained. *See* Exhibit 6, Transcript of Jail Call at 2 ("I've got some pictures of me and Kadra [sic] that are private and I think they are gonna look through um [sic]. . . .").

GLENN now claims that what he wanted disconnected were the uninterrupted power supply (UPS) batteries at his home. This claim is demonstrably false. A picture taken by law enforcement at the time of the Honduran search of GLENN's home clearly shows that the black box ***on top of the batteries*** is the Synology device. *See* Exhibit 7, Picture of Synology Black Box on Top of Batteries. Also, GLENN's recorded statement that he had private pictures in the Synology device that he did not want law enforcement to find, is at odds with GLENN's current position that he just wanted Sinia to unplug the batteries. One cannot store pictures in a battery. GLENN was clearly referring to the Synology storage device.

GLENN's attempt to tamper with evidence constitutes a second act of obstruction of justice meriting a two-level offense enhancement under Section 3C1.1. *See United States v. Ayerski*, 624 F.3d 1342, 1352 (11th Cir. 2010) (defendants engaged in child pornography sharing on the Internet who used encryption, changed nicknames and sharing groups, and software to avoid detection, obstructed justice by trying to thwart law enforcement investigative efforts);

United States v. Garcia, 208 F.3d 1258, 1261 (11th Cir. 2000) (reversed on other grounds) (defendant's instruction to an associate to destroy evidence is a basis for the obstruction of justice enhancement).

Additionally, GLENN's acts of deleting the log files from the SIPR hard drive after copying the stolen classified materials onto the DVD and his act of encrypting the stolen classified materials into a hidden compartment in the Synology device are similar to the obstructive conduct in *Ayerski*. Accordingly, the Court should also find that GLENN's deletion of the log files and encryption and secretion of the stolen classified materials on the Synology device to be two additional bases for obstruction of justice.

Finally, with respect to GLENN's plot to escape from Palm Beach Jail, the Government submits the report of interview of an inmate who claims that GLENN proposed an elaborate plot to escape from the jail to local safe houses, obtain false travel documents and travel to the Middle East. *See* Exhibit 13, FBI 302 Report of Interview of A.R.M.

Based on the substantial evidence of GLENN's attempt to obstruct justice by lying to the Government at his debriefing, attempt to tamper with the Synology device, deletion of the log files on the SIPR computer and encryption of the stolen secrets in a hidden compartment in the Synology device, the Court should deny his objection to paragraphs 38-40 and 48 of the PSI and accord GLENN a two-point enhancement for obstruction of justice.

GLENN also objects to paragraph 44 of the PSI, which sets his base offense level at 30 based on the two offenses of conviction, Counts 1 and 5, based on violations of 18 U.S.C. §§ 793(e) and 1030(a)(1), respectively. GLENN does not dispute that, with respect to his conviction of Count 5 under Section 1030(a)(1), the correct offense guideline is Section 2M3.2, Gathering National Defense Information, making his base offense level 30. Assuming

arguendo that the applicable guideline for § 793(e) is Section 2M3.3, GLENN's conviction of Count 5 under Section 1030(a)(1), still makes the applicable offense guideline Section 2M3.2, placing his base offense level at 30.

GLENN also objects to paragraph 47 of the PSI, according him a two-point offense level increase under U.S.S.G. § 3B1.3 for abuse of position of trust and use of special skill in the commission or concealment of his crimes. GLENN's argument that he lacked a special skill lacks any merit. Section 3B1.3 applies to defendants who employ a special skill in the form of a pre-existing, legitimate skill not possessed by the general public to facilitate the commission or concealment of a crime. U.S.S.G. § 3B1.3, Application Note 4; *United States v. Foster*, 155 F.3d 1329, 1331 (11th Cir. 1998) (printer employed a special skill in the crime of counterfeiting currency). However, the special skill enhancement also extends to defendants who commit their crimes through the use of unique technical skills not necessarily acquired through formal education. *Id.; United States v. Malgoza*, 2 F.3d 1107, 1111 (11th Cir. 1993) (expert radio operator employed special skill in drug smuggling conspiracy).

In the instant case, GLENN possessed special training and education in computer systems administration that allowed him to carry out complicated tasks such as implementing the Windows 7 operating system on the entire JTF-B unclassified and classified network. The highly technical skill required for this task is not the type of skill possessed by the general public. Moreover, GLENN has previously claimed to have an associate's degree in computer science and extensive technical computer security experience including: "Penetration (concealing activity from system log files). . . TCP/IP packet sniffing and logging. . . Keyboard logging. . . Social engineering. . . Mobile and landline telephone tricks (obtaining unpublished customer records, manipulation and cloning of ESN's, voice logging/recording, frequency scanning, etc.)".

See Exhibit 14, E-Mail Dated July 4, 2011. In that same email, GLENN touted his work at the Soto Cano Air Base working for Harris Corporation at the "Network Operations Center maintaining physical and virtual Windows servers and data backup applications." *Id*. at 3.

GLENN's crimes involved complex and highly technical tasks including: disabling Host Based Security System (HBSS) protections in a classified military computer system; erasing Windows security log files; creating a hidden compartment and encrypting the stolen materials. In short, GLENN employed more than special skills, but rather expert technical skills to hack, steal, and conceal the stolen military secrets. His special technical skills far surpass the special skills of the printer and radio operator found to be applicable in *Foster* and *Malgoza*.

Additionally, GLENN should be accorded a two-level enhancement for abuse of trust as a result of his crimes. As a system administrator at JTF-B, GLENN was entrusted with the security and integrity of the computer network. Indeed, he was trusted with creating and implementing the Windows 7 operating system image that would run the entire computer network. The trust that GLENN violated and abused was far more significant than that found to constitute obstructive conduct in other cases. *See, e.g.*, *United States v. Milligan*, 958 F.2d 345 (11th Cir. 1992) (postal clerk who embezzled post office funds); *United States v. Britt*, 388 F.3d 1369, 1372-73 (11th Cir. 2004), *reversed on other grounds*, (Social Security Administration part-time clerk abused her position of trust with respect to the victim – the government). *See also United States v. White*, 270 F.3d 356, 371 (6th Cir.2001) ("the general public may be victims of a government employee's crimes for purposes of deciding whether the employee's sentence may be enhanced pursuant to § 3B1.3").[4] GLENN should therefore be accorded a two-level enhancement for use of special skill and abuse of trust under Section 3B1.3.

[4] GLENN incorrectly cites *United States v. Harness*, 180 F.3d 1232 (11th Cir. 1999) for the

GLENN objects to paragraphs 48-49, 56-58 and 62 of the PSI calculating his total offense level based on his previous objections to the obstruction of justice and abuse of trust/special skill role enhancements and his claim of acceptance of responsibility. For all the reasons previously discussed, these objections should be denied.

GLENN also objects to paragraph 61 for failing to accord him a two-level reduction for acceptance of responsibility. Based on all of the obstructive conduct previously discussed and GLENN's continuous obstructive conduct and false statements, this objection should be denied.

GLENN objects to paragraphs 66-67 of the PSI detailing his "Other Criminal Conduct" including his misconduct in Iraq. For all the reasons previously discussed, this objection should be denied.

GLENN objects to paragraphs 73, 76, 81 and 99 of the PSI detailing his personal history. These paragraphs do not affect the calculation of the guidelines.

GLENN also objects to paragraphs 101 and 105 of the PSI for the calculation of his total offense level and his guidelines range based on his previous objections. For all of the reasons previously discussed, this objection should be denied. The correct total offense level is therefore 34 with a criminal history category of I, and GLENN's applicable guidelines range is 151-188 months of imprisonment.

C. The Section 3553 Factors

The United States respectfully recommends that the Court impose the statutorily authorized maximum sentence 120 months' imprisonment as to Counts 1 and 5 to run

---

proposition that the government cannot be the victim whose trust the defendant abuses under Section 3B1.3. *Harness* did not hold that. In fact, the court found in *Harness* that the victim there was the Red Cross, not the government. *Id*. at 1236. The Eleventh Circuit held in *Britt*, that the government was, in fact, the victim of the defendant's abuse of trust in that case and that the enhancement applied. 388 F.3d at 1273.

concurrently to each other, and 12 months of imprisonment as to Count 10, to run consecutively to Counts 1 and 5, which yields a combined sentence that is lower than the guideline imprisonment range of 151-188 months. The recommended sentence of 132 months is 19 months lower than the low end of the guideline imprisonment range and effectively constitutes a significant downward variance. In accordance with the factors listed in 18 U.S.C. § 3553(a), the United States recommends this sentence based on the need for the sentence imposed to: 1) reflect the seriousness of the offenses; 2) promote respect for the law; 3) provide just punishment for the offenses; 4) afford adequate deterrence to criminal conduct; and 5) protect the public from further crimes of the defendant, and 6) consider the applicable advisory Guideline range.

Sentence that Reflects the Seriousness of the Offenses

GLENN's criminal conduct was not a single mistake, but rather an elaborate pattern of willful and egregious criminal acts spanning several years. First, GLENN's immigration fraud conspiracy employed false statements, fabrication of false documents and fraud to apply for and ultimately obtain United States naturalization for his purported wife, KHADRAA. The immigration fraud conspiracy continued for years. In addition to creating fraudulent documents, GLENN coached KHADRAA to lie in her naturalization interview about where they lived and other facts that he believed could make her ineligible for naturalization. *See* Exhibit 15 at 3-4, 7, 8, Chats Between GLENN and KHADRAA; Factual Proffer (DE:101) at 15.

Not only was GLENN's pattern of misconduct with respect to the naturalization fraud conspiracy extensive and long-running, but his national security offenses also have a genesis that dates back several years before the conduct charged in Counts 1 and 5. Between March 2008 and January 2009, GLENN engaged in a pattern of misconduct while working as an independent contractor in Iraq. *See* Exhibit 10, CID Report. As a result of the extensive misconduct, the

Base Commander barred GLENN permanently from entering FOB Bucca in Iraq. *Id*.; Exhibit 12, Expulsion Letter.

After being expelled from Camp Bucca, GLENN moved to Australia with KHADRAA and became obsessed with gaining access to classified information. First, GLENN began to train himself on tradecraft that is typical of espionage. GLENN purchased a number of books on tradecraft including, among others: "The Official CIA Manual of Trickery and Deception"; "A Time to Betray"; "How to Disappear: Erase Your Digital Footprint, Leave False Trails, and Vanish Without a Trace"; "Surveillance Countermeasures": "A Serious Guide To Detecting, Evading, And Eluding Threats To Personal Privacy." *See* Exhibit 16, E-Mails Dated July 12, 2011.

Various email messages and chats between GLENN and KHADRAA dated between March and April 2012 also revealed that GLENN pressured KHADRAA to obtain a job as an intelligence analyst in order to obtain access to top secret (TS) classified information. *See, e.g*, Exhibit 17, E-Mail Dated April 10, 2012; Exhibit 18 at 3, Chat Dated March 15, 2012. In a March 15 chat, GLENN tells KHADRAA that if she can go to "Turkey and Palestine and Lebanon. . . meet with Syrians. . .**get intel**. . . you are. . .golden." [Emphasis added] *Id*. at 3. In another chat, KHADRAA asked GLENN what to tell her supervisor in an Australian government agency about whether her allegiance is to the U.S. or to Australia. GLENN replied: "[p]retty easy, whoever gives you a **TS clearance** gets the alligence [sic] right?" [Emphasis added] *See* Exhibit 19 at 4, Chat Between GLENN and KHADRAA. Another email during that time revealed that GLENN tried to spot and assess other contractors who had a top secret clearance, and therefore access to classified materials. *See* Exhibit 20, E-Mail Dated April 12, 2012. In that email, GLENN told the contractor "[i]f you have a **TS/SCI** [clearance]

already finalized, I might be in a good position to place you with a client who would need your skill set. . . ." [Emphasis added] *Id*.

In another particularly revealing email, GLENN touted his skills in: "**Penetration** (**concealing activity from system log files**). . . TCP/IP **packet sniffing and logging**. . . Keyboard logging. . . **Social engineering**. . . Mobile and landline telephone tricks (obtaining unpublished customer records, manipulation and cloning of ESN's, voice logging/recording, frequency scanning, etc.)". [Emphasis added] *See* Exhibit 14, E-Mail Dated July 4, 2011. Forensic analysis of GLENN's computers at JTF-B revealed that GLENN executed a packet sniffing and keyboard logging program on the JTF-B's system, which is essentially a wiretapping program. Additionally, GLENN's penetration into the JTF-B Commander's SIPR classified email account and GLENN's deletion of the JTF-B's secret computer system's log files are the types of hacking and concealment techniques that GLENN touted in his email. "Social engineering" is also a tradecraft technique that GLENN employed at FOB Bucca to persuade military personnel through lies, favors and cajoling to provide him access to the base's database systems, and to various goods and services to which he was not entitled.

The chats and emails described above put into context GLENN's motive and intent in committing his crimes. He engaged in a pattern of computer intrusion, theft of digital information, deceit, and fraud since 2008 when he was an independent contractor in Iraq. After his misconduct in Iraq was detected, he trained himself on espionage tradecraft techniques, obtained a system administrator position with the U.S. military in Honduras, and gained unauthorized access to highly sensitive military secrets, which he specifically targeted and stole. GLENN kept control of the stolen classified materials from June 17, 2012, until the search of his residence on March 11, 2014. During that nearly two year period, GLENN had the opportunity

to copy the DVD containing the classified information and deliver it to a foreign agent. GLENN also had the ability to give a foreign agent remote access to the Synology device. He never returned the stolen military secrets.

In fact, GLENN admitted in his debriefing with the prosecution team that he provided access to the Synology device containing stolen classified military plans and intelligence reports to two foreign associates, A.A. and Y.A.E. *See* Exhibit 8, FBI 302 Report of Interview, at 3. It is unclear whether these two individuals or someone else gained access to the stolen military secrets. Although GLENN denies that he gave anyone access, his pattern of surreptitious hacking, concealment of his crimes, obstruction of justice, false statements to law enforcement and obsession with obtaining classified materials suggests that GLENN is concealing his transfer of the stolen military secrets. All of these facts raise a reasonable inference that GLENN has transferred the stolen military secrets to an agent of a foreign power. Why else would he continue to lie about his crimes? The theft of military secrets along with the uncertainty and the inability to assess what damage GLENN has done to national security after his initial breach reflect the seriousness of his crimes. What we don't know about what GLENN did with the stolen military secrets heightens the gravity of his crimes.

Finally, the sensitivity of the information that GLENN stole brings into sharp focus the seriousness of his national security crimes. The classified materials that GLENN stole contained a number of intelligence reports and military planning documents that would cause serious damage to national security in the hands of a foreign adversary. The Court and the defense have been provided with a classified Declaration (Exhibit 21)[5] from Mr. James Baker,

5 Exhibit 21, as attached to this brief, is a redacted-unclassified version of the classified Declaration of Mr. Baker that has been served on the defense and filed separately, under seal and *in camera*, based on its classification and the sensitivity of the materials contained therein.

Principal Deputy Director for the Strategy, Policy and Plans Directorate of the Joint Chiefs of Staff at the Pentagon, which explains the significance of some of the most sensitive classified materials that GLENN stole and the potential serious damage to national security resulting from the breach.

Promote Respect for the Law

A total sentence of 132 months of imprisonment is significantly below the bottom of GLENN's guideline imprisonment range of 151 to 188 months. PSI ¶ 101. The fact that GLENN lied to law enforcement, his attempt to tamper with evidence and the egregiousness of his crimes further compel a significant sentence in this case. GLENN has demonstrated through years of criminal misconduct that he has no respect for the law. A sentence of 132 months' imprisonment is consistent with the § 3553(a) factor of promoting respect for the law.

Provide Just Punishment for the Offenses
And Consideration of the Advisory Guideline Range

GLENN has already received a significant reduction of his potential sentence as a result of his plea to only three of thirteen charged offenses. Pursuant to U.S.S.G., Section 5G1.2(d), "[i]f the sentence imposed on the count carrying the highest statutory maximum [which is 10 years in this case based on §§793(e) and 1030(a)(1)] is less than the total punishment [which is the guidelines range of 151-188 months in this case], then the sentence imposed on one or more of the other counts shall run consecutively, but only to the extent necessary to produce a combined sentence equal to the total punishment." After his plea and expected dismissal of other substantive counts, GLENN will receive at least a 19-month reduction from the bottom of his guideline range of 151 months simply by pleading guilty. Any additional reduction would

undermine two of the § 3553(a) factors, the need to provide just punishment and consideration of the advisory guideline range.

Afford Adequate Deterrence to Criminal Conduct

A sentence of 132 months will provide an adequate deterrence to other computer system administrators like GLENN who may pose an insider threat to national security. They will be on notice that the penalties for such criminal conduct will be serious. By contrast, any downward variance from the guidelines range would dilute the impact of our computer intrusion and espionage laws and would prove to be an insufficient deterrence to like-minded individuals who might be tempted to steal national security secrets.

Protect the Public from Further Crimes of the Defendant

GLENN has continued to lie to government agents and prosecutors and has withheld information about his theft of classified materials which make it more difficult to assess and counteract the damage he has done to national security. His crimes make him a continuing threat to society and to U.S. national security. The incapacitation of dangerous national security criminals like GLENN is one of the goals of the sentencing law as codified in this sentencing factor. *See* 18 U.S.C. § 3553(a)(2)(C). A sentence of 132 months of imprisonment will meet that goal.

Conclusion

Pursuant to the factors listed in Section 3553(a), and the applicable Sentencing Guidelines, the United States respectfully requests that this Court deny GLENN's objections and impose a combined sentence of 132 months of imprisonment, which is lower than the guideline imprisonment range.

Respectfully submitted,

WIFREDO A. FERRER
UNITED STATES ATTORNEY

By: *s/ Ricardo A. Del Toro*
RICARDO A. DEL TORO
Florida Bar No. 0957585
Assistant United States Attorney
99 Northeast 4th Street
Miami, Florida 33132-2111
Tel: (305) 961-9182
Fax: (305) 536-4675
Ricardo.Del.Toro@usdoj.gov

CHRISTIAN E. FORD
Trial Attorney
Counterespionage Section
National Security Division
United States Department of Justice
Tel: (202) 233-2049

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was filed by CM/ECF on July 10, 2015.

s/ Ricardo A. Del Toro
RICARDO A. DEL TORO
Assistant United States Attorney