

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION
LEXINGTON

UNITED STATES OF AMERICA,)	
)	
Plaintiff/Respondent,)	No. 5:12-CR-118-KKC-REW
)	No. 5:16-CV-304-KKC-REW
v.)	
)	RECOMMENDED DISPOSITION
IBRAHIMSHAH SHAHULHAMEED,)	
)	
Defendant/Movant.)	

*** **

Movant, Ibrahimshah Shahulhameed, is a federal inmate. DE #133 (Motion), at 1. On August 8, 2016,¹ Shahulhameed filed a *pro se*² motion, with an accompanying memorandum in support and appendix, under 28 U.S.C. § 2255. *See generally* DE ##133; 133-1, 133-2. The United States responded in opposition. DE #138 (Response). Shahulhameed replied, of sorts.³ DE #142 (Reply). The matter is ripe for consideration.

¹ This filing date reflects the prison mailbox rule. *See Richard v. Ray*, 290 F.3d 810, 812-13 (6th Cir. 2002) (*per curiam*). Here, Shahulhameed affirmed under penalty of perjury that he mailed the motion, per prison mail, on August 8, 2016. DE #133, at 9.

² *Pro se* petitions receive a comparatively lenient construction by the Court. *Franklin v. Rose*, 765 F.2d 82, 84-85 (6th Cir. 1985) (noting that “allegations of a *pro se* habeas petition, though vague and conclusory, are entitled to a liberal construction” including “active interpretation” toward encompassing “any allegation stating federal relief” (citations and internal quotation marks omitted)).

³ The Reply has many problems. First, it is unsigned, in general violation of the rules requiring a signature on all filings. *See* Fed. R. Civ. P. 11(a). Second, it is unverified, contrary to the particular requirements for § 2255 motions and supportive memoranda. *See* Rule 2(b)(5), Rules Governing Section 2255 Proceedings. As a matter of evidence, the unverified and unsigned tender is without weight or foundation. Next, the reply makes various arguments that appear for the first time—a reply may not properly raise new arguments. *See United States v. Turek*, Nos. 5:11-cr-29-JMH-HAI, 5:14-cv-7368-JMH-HAI, 2015 WL 5838479, at *6 (E.D. Ky. Oct. 6, 2015) (“It is well-established that a party, including a movant in a motion under § 2255, may not raise an argument for the first time in a reply brief.”). Finally, to the extent the reply tenders additional

Per normal practice, the District assigned the matter to the undersigned for a recommended disposition. The Court **RECOMMENDS** that the District Judge fully **DENY** § 2255 relief (DE #133) and issue **NO** Certificate of Appealability.

I. BACKGROUND INFORMATION

During the early morning hours of August 24, 2012, “Toyota experienced a cyberattack that rendered several of its computer servers inoperable.” DE #131 (Sixth Circuit Opinion), at 1. An internal investigation revealed that a user remotely accessed Toyota’s servers and issued commands affecting or altering computer code supporting multiple integral Toyota systems related to managing the flow of parts and the manufacturing process. *Id.* at 3. Until the night before the attack, Shahulhameed worked for Toyota as a contractor in the IT department, providing general support to Toyota’s IT infrastructure. Investigators determined that the harmful commands altering the code in question originated from Defendant’s Toyota-issued laptop and user ID in the early morning hours after Shahulhameed’s August 23 termination. *Id.* at 1-2. “Toyota employees spent 2,133 hours responding to the cyberattack between August 24 and October 30, 2012,” costing the company an estimated \$152,070 as a result of the intrusion. *Id.* at 6.

The United States, via FBI Special Agent Adam Keown, filed a criminal complaint and affidavit on September 18, 2012, charging Shahulhameed with violating 18 U.S.C. § 1030(a)(5)(A). DE #1 (Complaint). On October 4, 2012, a federal grand jury

documentary materials, those are not authenticated and thus not properly subject to consideration. *See Garcia v. United States*, Nos. 1:11CR253-3, 1:14CV150, 2015 WL 7283136, at *2 n.5 (M.D.N.C. Nov. 16, 2015) (collecting cases and holding unauthenticated documents not proper evidence in § 2255 proceedings). Although the Court endeavors to account fairly for all arguments presented, the Reply essentially is null, irrelevant, and without impact because of the multiple cited deficiencies.

indicted Defendant on the charge. DE #14 (Indictment). Shahulhameed went to trial, which lasted a full week.

The jury convicted on the sole count. DE #95 (Jury Verdict). Judge Caldwell sentenced Shahulhameed on June 4, 2014. DE #109 (Sentencing Minute Entry). Movant received a total prison sentence of 48 months followed by a 3 year term of supervised release. DE #111 (Judgment). Shahulhameed appealed, and the Sixth Circuit affirmed. DE #131. On August 8, 2016, Shahulhameed timely submitted a § 2255 motion to vacate. DE #133. The Government responded. DE #138. Shahulhameed replied.⁴ DE #142. The motion stands ripe for review. The Court wholly rejects each of Movant's claims.

Shahulhameed has failed to show any basis for relief. He groundlessly criticizes his retained lawyers for not challenging jurisdiction. He baselessly criticizes his lawyers

⁴ Shahulhameed prefaces his reply with fifteen alleged facts/issues on which the "Government is agreeing with defendant." DE #142, at 2-3. Per Shahulhameed, the United States does not contest these fifteen specific arguments or facts contained in his § 2255 motion; therefore, the Government agrees that defense counsel was ineffective in failing to investigate the listed issues. *Id.* Shahulhameed seems to assume that the Government must specifically rebut each allegation contained in the § 2255 motion or be deemed to have admitted same. He is mistaken. When ordered to respond, the Government need only "address the allegations in the motion." Rules Governing Section 2255 Proceedings, Rule 5(b); *see also Tarver v. United States*, 344 F. App'x 581, 583 (11th Cir. 2009) (refusing to apply Federal Civil Rule of Procedure 8(b)(6), which deems an allegation admitted if not specifically denied, in § 2255 context and holding: "[T]he government was not deemed to have admitted Tarver's allegation of ineffective assistance of counsel by failing to deny the allegation specifically in its response to his motion."); *United States v. Boniface*, 601 F.2d 390, 392-93 (9th Cir. 1979) (holding "the respondent's papers need only respond to the allegations of the motion" and need not satisfy the Civil Rules pleading requirements). Here, the United States thoroughly responded to the issues raised in the § 2255 motion, satisfying the Rule 5(b) response requirement. *See MacWilliams v. United States*, Nos. 1:08CV126, 1:06CR59-1, 2009 WL 6657795, at *20 (N.D. W.Va. Oct. 2, 2009) ("It is quite clear that Rule 5(b) does not require the respondent to respond to each and every separate claim individually. . . . [T]he respondent has in fact appropriately answered the allegations made in the petitioner's motion . . . none of the grounds have been conceded."). The Government has not conceded or admitted any of the claims advanced. Indeed, the Court treats the United States as contesting Shahulhameed's motion entirely; this technical and procedural gambit by Movant fails.

for not offering evidence, of unknown authenticity and dubious relevance,⁵ which would, even if used, have had no effect on the verdict. His other *Strickland*-based theories are similarly unavailing. For all of the reasons that follow, the District Judge should reject all claims.

II. STANDARD OF REVIEW

Under 28 U.S.C. § 2255, a federal prisoner may obtain post-conviction relief if his sentence violates the Constitution or federal law, the federal court lacked jurisdiction to impose such sentence, or the sentence exceeds the maximum authorized by law. 28 U.S.C. § 2255(a); *Mallett v. United States*, 334 F.3d 491, 496-97 (6th Cir. 2003) (“In order to prevail upon a § 2255 motion, the movant must allege as a basis for relief: ‘(1) an error of constitutional magnitude; (2) a sentence imposed outside the statutory limits; or (3) an error of fact or law that was so fundamental as to render the entire proceeding invalid.’” (quoting *Weinberger v. United States*, 268 F.3d 346, 351 (6th Cir. 2001))). A defendant alleging a constitutional basis must establish “an error of constitutional magnitude” and show that the error had a “substantial and injurious effect or influence on the proceedings” in order to obtain § 2255 relief. *Watson v. United States*, 165 F.3d 486, 488 (6th Cir. 1999) (citing *Brecht v. Abrahamson*, 113 S. Ct. 1710, 1721-22 (1993)). When alleging a non-constitutional error, a defendant must prove that the error constituted a “fundamental defect which inherently results in a complete miscarriage of

⁵ Notably, Shahulhameed’s proffered documents are not authenticated in any way. Thus, he tenders various papers, emails, and excerpts, but he does not describe or verify the source or foundation of those materials. The Court attempts to give fair review to each of Defendant’s claims. However, Movant has the burden here, and all evidence—to be evidence—requires proper verification. To the extent Movant attempts to prop his arguments on documentation, that documentation must be properly authenticated. That has not occurred in this record. Again, as noted previously, *see supra* note 3, the Reply is not even signed, doubly eroding the basis for consideration of reply-based materials.

justice,’ or, an error so egregious that it amounts to a violation of due process.” *United States v. Ferguson*, 918 F.2d 627, 630 (6th Cir. 1990) (quoting *Hill v. United States*, 82 S. Ct. 468, 471 (1968)); *see also Watson*, 165 F.3d at 488. In making a § 2255 motion, a movant generally bears the burden of proving factual assertions by a preponderance of the evidence. *McQueen v. United States*, 58 F. App’x 73, 76 (6th Cir. 2003) (*per curiam*) (“Defendants seeking to set aside their sentences pursuant to 28 U.S.C. § 2255 have the burden of sustaining their contentions by a preponderance of the evidence.”).

III. ANALYSIS

In his § 2255 motion, Shahulhameed nominally requests relief based on an allegation that the Court did not have subject-matter jurisdiction, DE #133, at 4-5, and on multiple allegations of ineffective assistance of counsel, *id.* at 3-4; DE #133-1. The Court had jurisdiction, and Shahulhameed warrants no *Strickland* relief. The nature of Shahulhameed’s arguments—all, besides jurisdiction, centering on evidence-based ineffective assistance arguments—required a full recanvass of the record. Thus, the Court read the entire trial transcript and reviewed each admitted exhibit. The Government proved at trial that Toyota’s IT subcontractor terminated Defendant late on August 23, 2012. Shahulhameed knew he was finished and was to have **no Toyota contact**. Despite that, in the wee hours of August 24, 2012, Shahulhameed repeatedly used his still-active Toyota computer access (via his Toyota-issued laptop and VPN password) to send commands to Toyota’s servers and/or make 50-60 changes in computer code, or other alterations, within Toyota’s computer systems. These changes impaired the affected servers and immediately disrupted Toyota’s operations. The objective proof tied all changes directly to Shahulhameed. Now, he contends his lawyers should have used a

series of temporally remote or unrelated documents to show that Shahulhameed typically had authority to make the changes at issue. He also makes a variety of other arguments critical of counsel's strategy or evidentiary choices. At the end of the day, whatever Shahulhameed's job at Toyota might otherwise or normally have been, the job was over on August 23, and any effort to claim authority to make injurious post-termination commands and coding changes is futile. Further, the changes hurt Toyota, were malicious, and plainly were in violation of 18 U.S.C. § 1030(a)(5). Defendant failed to prove any basis for *Strickland* relief.

A. *The Court had subject-matter jurisdiction over the indicted offense.*

Shahulhameed first argues: "Lack of Subject matter jurisdiction CFAA [Computer Fraud and Abuse Act] Statute does not applicable for 'Designer' and CFAA is an anti-hacking statute, not an employee misappropriation statute." DE #133, at 4 (all as in original). In the support memorandum, his elaboration on this claim, in its entirety, is as follows:

If the court determines at any time that it lacks subject-matter jurisdiction, the court must dismiss the action. "Because the CFAA is an anti-hacking statute, not an employee misappropriation statute And because the 18 § U.S.C. 1030 (g) statute guidelines clarifying clearly no action under this subsection for Designer/computer/software or hardware or firmware manufacture's negligent design."

DE #133-1, at 3 (all as in original).

Subject-matter jurisdiction is a court's "statutory or constitutional *power* to adjudicate the case." *United States v. Cotton*, 122 S. Ct. 1781, 1785 (2002) (quoting *Steel Co. v. Citizens for Better Env't*, 118 S. Ct. 1003, 1010 (1998)). Because it involves a court's ability to hear a case, challenges to subject-matter jurisdiction "can never be forfeited or waived," and defects "require correction regardless of whether the error" was

previously raised. *Id.* Federal district courts have subject-matter jurisdiction over all federal crimes. 18 U.S.C. § 3231. “To invoke that grant of subject matter jurisdiction, an indictment need only charge a defendant with an offense against the United States in language similar to that used by the relevant statute. That is the extent of the jurisdictional analysis: [A] federal criminal case is within the subject matter jurisdiction of the district court if the indictment charges . . . that the defendant committed a crime described in Title 18 or in one of the other statutes defining federal crimes.” *United States v. Scruggs*, 714 F.3d 258, 262 (5th Cir. 2013) (footnotes, citations, and quotation marks omitted); *see also United States v. Henry*, 12 F.3d 215, Nos. 92-6649, 92-6650, 92-6653, 1993 WL 492302, at *3 (6th Cir. 1993) (table) (“Title 18 U.S.C. § 3231 vests federal district courts with jurisdiction over offenses against the laws of the United States. The defendants were charged with making false statements to the United States government. The district court therefore has jurisdiction to hear this case.”).

Here, the Indictment charged that Shahulhameed “knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage, without authorization, to a protected computer,” and said “course of conduct affecting one or more protected computers caused loss to a person, during a one-year period, aggregating at least \$5,000 in value[,]” in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i). DE #14, at 1. The Indictment charged a federal crime and tracked the language of the underlying statute. The District Court plainly had subject-matter jurisdiction.

Shahulhameed’s argument fundamentally misunderstands the function of subject matter jurisdiction. In advancing the jurisdictional argument, he actually argues that the

United States could not have charged him with a crime under the CFAA because he, a subcontractor who provided tech and design support for various web-based applications at Toyota, was exempt from such action as a “designer.” Defendant’s core argument centers on 18 U.S.C. § 1030(g), which creates a civil cause of action under the CFAA. Shahulhameed relies on the following sentence in particular: “No action may be brought under this subsection [§ 1030(g)] for the negligent design or manufacture of computer hardware, computer software, or firmware.” 18 U.S.C. § 1030(g). He argues that his employment contract with Toyota required him to design, install, and support various Toyota web configurations. DE #133-1, at 4. He cites and attaches a letter from Toyota allegedly outlining his job responsibilities: “Mr. Shahulhameed’s detailed day-to-day duties and responsibilities as a Programmer Analyst include involvement in developing and supporting Toyota’s e-business Web and Data Management databases. Mr. Shahulhameed has been specifically responsible for *design* of web configuration, installation, administration, and support of Toyota’s standard web application servers.” DE #133-2 (Appendix), at 9 (emphasis added). Shahulhameed contends that any changes to the servers attributable to him simply arose from the “negligent design or manufacture” of code, exempting him from liability under § 1030(g). DE #133-1, at 5.

As mentioned above, however, § 1030(g) creates a *civil* cause of action for persons who suffer damage or loss resulting from a CFAA violation. It does not modify or apply to criminal liability under the CFAA. The plain language of the statute supports this reading. Subsection (g) begins: “Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator[.]” 18 U.S.C. § 1030(g). Although the CFAA is primarily a criminal statute, as evidenced by its

placement in Title 18, subsection (g) creates a civil cause of action for afflicted persons, a reading supported by various courts. *See, e.g., Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1072 (6th Cir. 2014) (referencing § 1030(g): “The CFAA is primarily a criminal statute, but it provides for a civil right of action and economic damages in certain circumstances[.]”). Further, the statute specifically cabins the language on which Shahulhameed relies. The negligent design limitation applies only to actions “brought under this subsection,” *i.e.* civil actions. Accordingly, under a plain language interpretation, section 1030(g) does not limit the criminal provisions of the CFAA. Here, the United States brought criminal charges, via a criminal indictment, against Shahulhameed for violating 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i). Subsection (g) offers Shahulhameed no recourse to challenge jurisdiction⁶ as to the criminal prosecution.⁷

⁶ The Court need not parse the new arguments of the unsigned Reply; none addresses the fundamental difference between a § 1030(g) civil action (which is the argument thrust) and **criminal** jurisdiction.

⁷ Likewise, counsel did not provide ineffective assistance by not analyzing or making a jurisdictional challenge. *See* DE #133-1, at 4-5 (Movant arguing counsel failed to investigate the § 1030(g) argument), 54 (Movant arguing counsel should have filed a motion to dismiss). Counsel need not make futile arguments to satisfy the Sixth Amendment. *See Greer v. Mitchell*, 264 F.3d 663, 676 (6th Cir. 2001) (“By definition, [] counsel cannot be deemed ineffective for failure to raise an issue that lacks merit.”); *see also United States v. Latham*, No. 1:07-cr-270, 2010 WL 161436, at *4 (W.D. Mich. Jan. 8, 2010) (collecting cases and stating: “As a matter of law, one cannot render constitutionally ineffective assistance of counsel by ‘failing’ or refusing to raise arguments which lack merit, whether at trial or on appeal.”). For all the reasons stated above, any ineffective assistance claim based on Shahulhameed’s proffered analysis of § 1030(g) fails. In this criminal context, a motion to dismiss based on the civil cause of action statute would have been futile. Further, a motion to dismiss, as to contested factual matters, likewise would have been improper. *See Universal Milk Bottle Serv. v. United States*, 188 F.2d 959, 962 (6th Cir. 1951) (holding a motion “claiming that [the indictment’s] allegations are false and untrue” improper because “issues of fact” must “be tried by a jury”); *United States v. Levin*, 973 F.2d 463, 467 (6th Cir. 1992) (holding a Rule 12 motion inappropriate if it requires the court to “invade the province of the ultimate finder of fact”). Again, Shahulhameed gets no relief on these bases.

B. *Shahulhameed's ineffective assistance of counsel claims fail.*

Shahulhameed next makes several IAC arguments. When asserting an ineffective assistance claim, a movant must prove both deficient performance and prejudice. *Strickland v. Washington*, 104 S. Ct. 2052, 2064 (1984); *Campbell v. Bradshaw*, 674 F.3d 578, 586 (6th Cir. 2012); *Pough v. United States*, 442 F.3d 959, 964 (6th Cir. 2006) (noting that a movant must prove ineffective assistance by a preponderance of the evidence). In order to prove deficient performance, a movant must show that “counsel made errors so serious that counsel was not functioning as the ‘counsel’ guaranteed the defendant by the Sixth Amendment.” *Strickland*, 104 S. Ct. at 2064. A movant meets this burden by showing “that counsel’s representation fell below an objective standard of reasonableness” as measured under “prevailing professional norms” and evaluated “considering all the circumstances.” *Id.* at 2064-65. Judicial scrutiny of counsel’s performance, however, is “highly deferential,” featuring a “strong presumption that counsel’s conduct falls within the wide range of reasonable professional assistance[.]” *Id.* at 2065.

Deficient performance is considered constitutionally prejudicial only when “counsel’s errors were so serious as to deprive the defendant of a fair trial, a trial whose result is reliable.” *Id.* at 2064. In order to prove prejudice, a movant “must show that there is a reasonable probability that, but for counsel’s unprofessional errors, the result of the proceeding would have been different.” *Id.* at 2068. When evaluating prejudice, courts generally must take into consideration the “totality of the evidence before the judge or jury.” *Id.* at 2069. Finally, courts need not address counsel performance prior to

assessing any prejudice suffered “if it is easier to dispose of an ineffectiveness claim on the ground of lack of sufficient prejudice.” *Id.* at 2069.

Shahulhameed here raises a host of *Strickland* assertions, most of which claim prejudice from defense counsel’s failure to introduce various documents or make certain arguments. His overarching theme is most clearly articulated at the end of the unsworn reply. The Court quotes Movant’s original language:

Defendant’s counsel was not deficient on rendering service to assumptions and theories, he gave the government a reasonable battle on these different assumptions and theories, he did not fail, instead, he failed as defendant’s counsel when he forgot to identified the “Hard Evidence” that goes beyond any overwhelming evidence that is based on assumptions and theories, therefore, he forgot to fulfill the interest of justice and prejudice defendant.

Defendant’s counsel forgot that “Hard Evidence” is accurate and do not need witnesses; most of the time the relevant part of a case is based in witnesses because there are no contracts, subcontracts, legal descriptions and/or documents that legally manage or established the work performance, but in this case the **“Hard Evidence” CAN NOT BE IGNORED** because is based on **LAW**.

DE #142, at 23. The Court has read the entire record, including the full trial transcripts. Counsel provided a vigorous defense and reasonably refrained from introducing the complained of particular pieces of “hard evidence.” Defendant likewise failed to demonstrate any resulting prejudice. In order to avoid second-guessing trial counsel’s strategic decisions, “a court must indulge a strong presumption that counsel’s conduct falls within the wide range of reasonable professional assistance; that is, the defendant must overcome the presumption that, under the circumstances, the challenged action might be considered sound trial strategy.” *Id.* at 689, 104 S. Ct. 2052 (internal quotation marks and citation omitted). Accordingly, “an ineffective-assistance-of-counsel claim cannot survive so long as the decisions of a defendant’s trial counsel were reasonable,

even if mistaken.” *Campbell*, 260 F.3d at 551; *Moss v. Hofbauer*, 286 F.3d 851, 859 (6th Cir. 2002). Shahulhameed’s ineffective assistance claims wholly fail.

Before evaluating specific theories, the Court makes a few unavoidable and foundational observations from the record.

First, the United States conclusively proved that Shahulhameed knew he had been fired on the evening of August 23, 2012. The contractor’s representative, Andrew Sell testified as such, and Exhibit 1, an email, inarguably informed Movant that he was finished at Toyota: “you should NOT have any future contact with . . . anyone at Toyota.” When all hell broke loose on Toyota’s systems the next morning and an unwitting IT manager reached out to Shahulhameed, he immediately responded that he was “no longer working for Toyota.” DE #126 (Trial Transcript, Day 2), at 59 (Veerasamy testimony).

Second, Shahulhameed offering proof of typical, historical, or other duties he might have performed over time hardly informs whether he had authority to take any steps at Toyota past the witching hour; he had been fired and told to have no contact with Toyota as of late on August 23. Despite that, he repeatedly entered Toyota’s systems through the night. On a recorded call that Friday morning (August 24), as Toyota tried to get a handle on the problems, Shahulhameed claimed only to have taken “backups” from the system. *Id.* at 195-197. As to whether he had made *any* changes, just hours before, Shahulhameed responded: “Not that I remember. Not that I remember.” *Id.* at 199. Thus, his story at the time, mere hours after the fact, was that he had only made backups and had no recollection of making changes. This strongly colors the Court’s view of any suggestion now that Shahulhameed was properly or legitimately altering the Toyota systems post-termination.

1. Failing to introduce evidence that Shahulhameed had authorization to make changes (Arguments 2, 3, and 11)

Shahulhameed makes several related ineffective assistance of counsel arguments centered on defense counsel's supposed failure to demonstrate at trial that Defendant had authorization to make the programming changes at issue. *See* DE #133-1, at 7-25, 50-53. Specifically, he faults counsel for failing to introduce certain documents purportedly showing that (1) he had authority to make the specific types of changes at issue, (2) he had not actually been fired the night of August 23, 2012, as alleged, and (3) he had authorization to fix problems with the Toyota system.

Shahulhameed's authorization, or lack thereof, to make the damaging changes to Toyota's systems was a central issue at trial. *See* DE #129 (Trial Transcript, Day 5), at 16 (United States closing argument), 22-30 (Defense closing argument). To obtain a conviction under the CFAA as charged, the United States had to prove that Shahulhameed "intentionally cause[d] damage *without authorization*, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (emphasis added). On direct appeal, the Sixth Circuit succinctly defined "authorization," a term undefined within the CFAA, as something requiring "approval or sanction." DE #131, at 3 (citing *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012)). The Sixth Circuit summarized the evidence presented at trial:

The evidence also shows that Shahulhameed acted without authorization. . . . Andrew Sell, a technical recruiter for GlobalSource IT, testified that he received a call on August 23, 2012, from Adi Gimpaunu, a GlobalSource contractor working for Toyota, stating that Shahulhameed had harassed Gimpaunu by demanding that Gimpaunu pay Shahulhameed a "finder's fee," or something to that effect. Managers at Toyota heard about the incident and called GlobalSource that evening, stating that one of the two contractors had to be removed. Sell called Shahulhameed on the evening of August 23, 2012, and "told him that the decision has been made that

your project has been terminated, that you should have no contact with anyone at Toyota, [and] that you should not report to Toyota tomorrow morning, the next day.” Sell asked if Shahulhameed understood, and Shahulhameed said, “yes, okay.” Sell also sent Shahulhameed an e-mail that same evening clarifying that he should not report to work the next day and that he should not have contact with anyone at Toyota. Shahulhameed testified that he received the e-mail and replied to it.

Shahulhameed argues that his access was authorized because Toyota did not disable his user account until at least eight hours after his conversation with Andrew Sell. But Toyota's failure to disable his account does not mean that his access was authorized; the phone call and email from Sell are sufficient to establish a lack of authorization. Given the late hour—Sell e-mailed Shahulhameed around midnight—it is not surprising that Toyota waited until the next business day to disable his account.

DE #131, at 2-3.⁸

Despite this strong proof and clear finding by the Sixth Circuit, Shahulhameed chides his lawyers for not proving up his typical IT duties, not contesting the legal authority to fire, and not making other technical computer-based or sequence of conduct claims. The Court has read everything and sees no reason to question the lawyers' performance or strategy. More fundamentally, the evidence Shahulhameed touts would not reasonably have affected the verdict.

a. Documents purportedly showing specific changes authorized

Shahulhameed first argues that his attorneys were ineffective for failing to introduce several documents purportedly showing that Toyota had generally authorized Defendant to make the specific programming changes attributed to him at trial. Shahulhameed identifies five areas where counsel failed to tender documents allegedly showing his authorization to: (1) make changes to security certificates (security.xml file changes); (2) delete security.xml files; (3) change timestamps on files; (4) implement

⁸ The status of Toyota's servers as “protected computer[s],” per § 1030(e)(2)(B) is inarguable given the commercial context of the electronics and Toyota's interstate, indeed international, manufacturing model.

changes to the Oracle Business Intelligence (OBIEE) system; and (5) change the connector names of configuration files. *See* DE #133-1, at 7-22. He identifies five particular documents that counsel did not introduce at trial, including a document titled “Roles and Responsibility Descriptions” and several emails purportedly supporting his authorization to make the changes in question. *Id.* The United States responded in opposition. DE #138, at 12-14. Shahulhameed’s argument fails.

None of the documents⁹ Defendant tenders with the § 2255 motion or reply demonstrates that Shahulhameed had authorization, *i.e.*, approval or sanction, to execute the changes made on August 24, 2012. For example, Shahulhameed tenders a document titled “Roles and Responsibility Descriptions,” dated October 15, 2011. DE #133-2, at 11-18. It purports to outline various responsibilities applicable to Shahulhameed as an IT contractor/administrator for Toyota. *Id.* The document, in part, states that there is “[n]o need for management approval to run” security certificate checks and that “[r]unning certificate check is part of day to day activity[.]” *Id.* at 15. Shahulhameed also points to the document as granting approval to delete server index files, *id.* at 13, and change various file timestamps, *id.* at 15 (“invalidate the cache by changing the time stamp”).

These “Roles and Responsibility Descriptions,” however, only nominally apply to the “current websphere development issue” on server “T00TSA20D.” *Id.* at 11. Per Shahulhameed’s own testimony at trial, the T00TSA20D server “is a non-production server. That means it is a playground server for everybody. And this is a server we use it, like if any new tool come to the market[.]” DE #128 (Trial Transcript, Day 4), at 113. Shahulhameed’s supervisor at Toyota, Tom Cantrell, similarly described non-production

⁹ Again, Movant provides no foundation or authentication for any of the records. Appendix 3 is riddled with typos, mismatched fonts, and odd verbiage, raising doubts about its provenance.

or development servers as “kind of like a playground for the people that are developing the screens and the buttons and all of those things that offer up to the users. That’s where they go to test and play so that they can see for themselves that it works or doesn’t work before it gets promoted on up through the — to the production environment.” DE #125 (Trial Transcript, Day 1), at 49. The permissive nature of changes to a development environment, for example, as outlined in the “Roles and Responsibility Descriptions,” differs significantly from the stringent change process for production or client-facing servers, as detailed by Tom Cantrell at trial. *See, e.g., id.* at 47-49 (describing changes as taking “approximately two weeks to get through that change control process because it has to get all the proper approvals”). As demonstrated by the trial testimony, the free range granted programmers to make changes in development spaces does not apply to the type of client-facing programs, *e.g.*, ToyotaSupplier.com, affected by the changes the night of August 23 and morning of August 24. Accordingly, the “Roles and Responsibility Descriptions” document, which focuses on one of these non-production servers, has little bearing on whether Shahulhameed normally would have had authority to make changes to production-level servers. Mr. Cantrell testified unequivocally, DE #126, at 15-16, that Shahulhameed did not have blanket authority (or authority particular to that night) to make such changes; nothing Movant offers counters that assessment.

Similarly, Shahulhameed does not rationally relate the various emails he attaches to the § 2255 motion and in reply to the August 24 conduct. *See* DE ##133-1, at 19-20, 22; 133-2, at 23-26, 28-30, 32; 142-1, at 2-5, 7-10. He claims that the attached emails evidence prior approval for the changes made on August 24. However, the emails, primarily sent by Shahulhameed to other IT professional at Toyota, discuss programming

changes occurring prior to the August 24 cyberattack, mostly relating to changes implemented in the first half of 2012.¹⁰ *Id.* Even the two August 2012 emails discuss changes prior to the August 24 damaging conduct. *See* DE #133-2, at 25-26, 32. Nothing on the face of these documents grants approval for changes during the early morning hours of August 24.

Given the attenuated relationships between the tendered documents and the unauthorized transmission of damaging computer code at issue, Shahulhameed has not shown how counsel performed deficiently by failing to use these documents at trial. Further, the defense's overarching trial strategy indeed involved establishing that Shahulhameed *had authority* to make the August 24 changes. DE #129 (Defense Closing Argument), at 26 ("So there's no reason to think that Mr. Shahulhameed was without authorization, that he was of the opinion that he could not continue to do what he's always – he had always done[.]"). Defense counsel elicited from Defendant's former supervisor Cantrell that Shahulhameed did not, under certain circumstances, need prior approval to work from home and that he made various file changes as part of his routine duties. DE #126, at 24-25, 32-33. Shahulhameed testified to his day-to-day responsibilities, which he stated included making many of the pertinent programming changes as a matter of routine. *See* DE #128, at 54-56 (updating security certificates), 66 (changing timestamps), 71-75 (deleting unneeded files), 81-89 (modifying server configuration files), 103-04 (adding and removing certificates from OBIEE). With counsel having prompted testimony on cross-examination and from Shahulhameed on

¹⁰ In fact, two of the email chains show Shahulhameed following the formal change approval process described by Cantrell during his testimony at trial. DE #142-1, at 2-5, 7-10; *see also* DE #125, at 53-54. None of the documents presented shows similar change authorization relating to the August 23 and 24 changes.

direct regarding his apparent authority to make the specific changes at issue, Shahulhameed does not show deficient performance for failing to introduce these additional documents, which simply do not add meaningfully to the argument that Defendant had authority to make the August 24 changes. While the record does not reveal counsel's exact thought process as to these documents, Shahulhameed does not rebut "the strong presumption that [counsel excluded the documents] for tactical reasons rather than through sheer neglect." *Yarborough v. Gentry*, 124 S. Ct. 1, 5 (2003) (further stating that the presumption "has particular force where a petitioner bases his ineffective-assistance claim solely on the trial record"). Especially given the highly technical record, deciding not to introduce these documents of limited relevance to the conduct at issue, especially in the face of more pointed witness testimony elicited from Shahulhameed and on cross-examination, was surely defensible lawyer strategy.

Even if counsel erred in not introducing the specific documents cited, Shahulhameed cannot establish prejudice. The Government presented evidence at trial establishing that GlobalSource IT terminated Shahulhameed's project with Toyota on August 23, 2012, robbing him of *any* authorization as to Toyota's systems. Andrew Sell, a recruiter for GlobalSource IT, testified that he called Shahulhameed on the night of August 23 and "told him that the decision has been made that your project has been terminated, that you should have no contact with anyone at Toyota, that you should not report to Toyota tomorrow morning, the next day, and asked him if he understood; and he said yes, okay." DE #125, at 9. The Government introduced an email (Exhibit 1) from Sell to Shahulhameed that confirmed their conversation. *See id.* at 10-13; DE #138-1, at 1. Additionally, Toyota employee Veerasamy testified that, when he called Defendant for

assistance the morning of August 24, Shahulhameed informed him “As of last night, I’m no longer with Toyota.” DE #126, at 59. As noted above, the documents here presented all pertain to purported authorizations granted for changes made *prior* to the cyberattack and Shahulhameed’s separation from Toyota. They do not counter the predominant evidence presented at trial that Shahulhameed, as a fired contractor, had no authorization even to access the systems, much less to make the programming changes charged.¹¹ The fact that the changes hamstrung Toyota’s servers, and thus were plainly harmful to the entity, shouts loudly that Toyota gave Shahulhameed no authority for such acts. Accordingly, he suffered no prejudice by any failure to introduce the documents.

To this, the Court must add an overlay of common sense. The Court has no doubt that Shahulhameed, when employed, had authority to do his job at Toyota. That may have involved particular maintenance-related tasks in particular environments, as suggested in his proffered papers. That may have involved specific code changes at times. The question of Shahulhameed’s general job duties is very different from an assessment of what he did in the early morning of August 24, a time when he had been fired and had no business being on Toyota’s system. As a former employee, he acted as an electronic trespasser and had no employment authorization at all.

¹¹ Shahulhameed also obliquely argues that counsel used an improper “without authorization” standard governing his conduct. DE #142, at 11. Shahulhameed particularly references Judge Caldwell’s order denying the motion for acquittal (DE #104). There, Judge Caldwell found defense counsel improperly conflated authorized access with authorization to use such access to transmit code. The two are indeed distinct. *See, e.g., Cheney v. IPD Analytics, L.L.C.*, No. 08-23188-CIV, 2009 WL 1298405, at *7 (S.D. Fla. Apr. 16, 2009) (“Therefore, the fact that Calkins may have had initial authorization to *use* the computer does not immune him from liability under subsection 1030(a)(5)(A) for *causing damage* to the computer.”). However, though counsel may have compressed the two standards in the motion for acquittal, defense counsel prompted testimony, from Shahulhameed and on cross-examination, that the code transmissions attributed to Shahulhameed were authorized. The defense did present proof on Shahulhameed’s authority with respect to changes at issue.

Further, Toyota’s witnesses testified in detail to a sample of the changes that occurred on the target night. There were 50-60 total changes made, all of which Toyota’s inside and outside experts, and the FBI, placed on Shahulhameed. *See* DE #126 (Veerasley testimony), at 60-87 (describing diagnosed changes); *id.* (Siebert testimony) at 232-50 (describing changes and attribution to Defendant); DE #127 (Trial Transcript, Day 3 – Siebert testimony continued) at 31-32, 39, 107-09; *id.* (Hall testimony) at 176-88 (attribution); *id.* (FBI Agent Keown) at 202, 206 (attribution). The changes dramatically impacted Toyota’s systems (15-20 systems, per Siebert, DE #126, at 39), which is why the company rang the alarm bell early on August 24. While Shahulhameed might attempt to describe certain changes as benign, he does nothing to undercut the basic facts of the night—Shahulhameed’s unique laptop and unique ID accessed the system for four sessions and authored a series of changes that immediately and sharply impaired Toyota’s computers. Normal maintenance, taking of backups, and benign presence on the system would not, quite obviously, have introduced the damage traced directly to Shahulhameed’s commands. With or without Shahulhameed’s “hard evidence,” this is the compelling, and inarguably incriminating, truth from the record.

b. Documents purportedly showing Shahulhameed remained employed/authorized to work at Toyota on August 23/24

Shahulhameed next argues defense counsel was ineffective for failing to introduce two documents purportedly showing that Defendant was not fired. He claims that “there was no form of communication provided to defendant of being fired and hence defendant was unaware that he was not permitted to log on to the system.” DE #133-1, at 23. He contends that the two documents, the contract between GlobalSource IT and Genome International and an email sent to Shahulhameed by GlobalSource IT following his

termination, support his claim that GlobalSource IT did not, at the critical time, fire him. *Id.*; DE #133-2, at 2-7, 34. According to Shahulhameed, these documents, properly presented, could have allowed a “reasonable Jury [to find] that defendant was not fired on the evening of August 23/24, 2012.” DE #133-1, at 24. Defense counsel’s failure to present these documents “so under minded [sic] that proper functioning of the adversarial process that the proceeding cannot be relied on as having produced a just result.” *Id.* The United States responded in opposition. DE #138, at 14-15.

Defendant’s argument fails.¹² Again, as above, the documents Shahulhameed relies on do not address his “approval or sanction” to make the damaging changes to Toyota’s system. Shahulhameed argues that counsel deficiently performed by not presenting the contract between GlobalSource IT, the contractor engaged by Toyota to provide contract labor, and Genome International, a subcontractor and Shahulhameed’s direct employer. Defendant argues that the contract required GlobalSource IT “to terminate the contract with Defendant’s employer [Genome] who have authority to deny authorization to work with client [Toyota].” DE #133-1, at 23 (all as in original). As such, per Shahulhameed, GlobalSource IT, via Andrew Sell, did not have power to terminate him the evening of August 23—only Genome, his direct employer, possessed that right.

¹² Nor does the late-day email from August 24 effect the post-firing authorization. *See* DE #133-1, at 25. GlobalSource IT would have allowed Shahulhameed to help after the fact, at Toyota’s request. This willingness sheds no light on Movant’s status between his firing and the cyberattack. Defendant’s own e-mail shows that this issue arose only after Toyota’s phone call directly to Shahulhameed, when Toyota was beginning to grapple with the night’s events.

Shahulhameed does not show how counsel's failure to introduce this contract equates to deficient performance.¹³ True, the contract does state that the relationship between GlobalSource IT and Genome will "remain in effect until properly terminated" and that either party "may terminate this Agreement on 30 days written notice." DE #133-2, at 4. The contract further calls for all notice to be "in writing" and sent "by certified or registered mail." *Id.* at 7. However, GlobalSource IT could terminate the contract "immediately in the event that the Customer [*i.e.*, Toyota] no longer desires to use the services or personnel provided by Subcontractor[.]" *Id.* at 4. Additionally, nowhere does the contract state that Genome retains the sole ability to remove the employee (in this case Shahulhameed) from the authorized position at Toyota. Whatever Genome's rights as to GlobalSource IT, Toyota controlled its own property and had the undisputed right to regulate access. It told GlobalSource IT to remove one of the IT workers, and GlobalSource IT chose Defendant. *See* DE #125, at 8-9. Sell, for GlobalSource IT, terminated Shahulhameed. *Id.* The contract, whatever its worth, does not speak to or limit this course of events.

c. Additional documents purportedly showing Shahulhameed's general authorization to perform changes

Shahulhameed finally argues, in a disjointed manner, that counsel failed to establish his general authorization to make the changes at issue and GlobalSource IT's motive to frame him for Toyota's damage. DE #133-1, at 50. The United States responded in opposition. DE #138, at 24.

Regarding his authorization, Shahulhameed states:

¹³ Additionally, defense counsel elicited similar information during cross-examination of Andrew Sell, the GlobalSource employee who terminated Shahulhameed the night of August 23. Sell confirmed that Genome, not GlobalSource, directly employed Defendant. DE #125, at 18.

[D]efendant fixed problems created by Devadass Veerasamy (see Appendix no. 16) or anybody else in Toyota, that's why he was hired and contract extended for another year as "Programmer Analyst" to performed under the scope of these duties and responsibilities when something was going wrong with Toyota's system.

DE #133-1, at 50 (all as in original). Shahulhameed attaches an email exchange that appears to be an example of Shahulhameed fixing an issue on a Toyota server system on August 13, 2012. *Id.* at 51-52. The email exchange, reflecting historical work responsibilities, has no bearing on Shahulhameed's post-termination authorization on Toyota's systems. Further, as previously addressed above, defense counsel's trial strategy specifically included argument that Shahulhameed had authorization to enact the changes central to the case as part of his day-to-day responsibilities. Shahulhameed testified as such. DE #128, at 54-56, 66, 71-75, 81-89, 103-04. Counsel went further and elicited testimony on cross-examination that Toyota supervisors and coworkers thought Shahulhameed a great employee, ready to go above and beyond the call of duty, and relied on him to fix various IT issues. *See, e.g.*, DE #126 (Cantrell Testimony), at 23 ("Q: And you would agree with me before all this allegedly occurred, I'll use that word, he was a great employee? A: Definitely, yes.").

Movant also seems here to be arguing about contract mechanics and GlobalSource IT's motive to blame Shahulhameed. The Court sees nothing persuasive here and finds it implausible to think that GlobalSource IT would get any advantage from its sub-contractor (or anyone else acting for GlobalSource IT) bearing responsibility for \$180,000 in damage to its client. The tendered argument, of most dubious logic, would have no impact on the jury's verdict.

2. Failing to produce evidence of ToyotaSupplier.com's availability (Argument 4)

Shahulhameed further argues that counsel failed to produce evidence that ToyotaSupplier.com was accessed several times the morning of August 24 (after the cyberattack). DE #133-1, at 26-30. Defendant specifically argues that counsel did not introduce certain web server logs and browser logs purporting to show that the website was operational. *Id.* Shahulhameed asserts that this evidence of website operation refutes any evidence at trial showing that Toyota suffered damage as a result of any coding or command by Movant. *Id.* The United States responded in opposition. DE #138, at 16.

This argument conclusively fails. Defense counsel in fact substantially used the evidence at trial Shahulhameed claims was omitted. During the cross-examination of Dennis James Siebert, Jr., Toyota's forensic examiner, counsel introduced excerpts from the browser history for ToyotaSupplier.com that appear to show a computer accessed the website at 6:38 a.m., 8:19 a.m., and 8:20 a.m. DE #127, at 75; Defense Exhibit 7. This document coincides with the document presented by Shahulhameed on page 30 of DE #133-1. Counsel questioned Siebert about the document's contents in an attempt to reflect ToyotaSupplier.com's availability. While Siebert's testimony on cross-examination disagreed with the defense's interpretation of the document in question, *see* DE #127, at 75 (in response to question regarding website being accessible per document: "The – from what I'm reading here, it would have said [only] the portal was accessed."), the jury saw the document in question and the cross-examination framed the issue Shahulhameed here claims counsel failed to appropriately raise. Shahulhameed could suffer no prejudice resulting from counsel's failure to submit certain evidence or make

certain arguments when counsel *did in fact* present the identified evidence and make the identified arguments. Shahulhameed's fourth argument fails.

Further, and again, the case was about damaging commands and code, and the Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The cumulative testimony included reported corruption of code in or negative changes affecting 15-20 systems via 50-60 modifications implemented by Shahulhameed. Further, the inoperability or negative performance of the TS website is exactly what started the reactive ball rolling on the morning of August 24. To claim the system operated properly despite Shahulhameed's conduct is to ignore the conclusive weight of the full record. *See* DE #126 (Berberian testimony), at 201-02 (reporting ToyotaSupplier.com as "down" and that "no one could log in internal or external" and further listing other affected systems).

3. Failing to properly challenge Toyota damages and the investigation linking Shahulhameed to harmful changes (Argument 5)

Via a series of arguments, Shahulhameed claims his lawyers failed to challenge assumptions about Toyota damages, failed to contest invalid file comparisons, and failed to dispute the non-effect of "port" changes. DE #133-1, at 31-37. These theories have no validity. The defense strongly criticized the underlying investigation and Toyota's failure to preserve certain file evidence. *See* DE #127 (Siebert testimony), at 69-70 (reports not based on forensic images of networks); *id.* at 94-98 (cross-examination regarding manipulability of configuration file comparisons); DE #128 (Keown testimony), at 10-11 (FBI relied on Toyota reports and investigation). As to damage assumptions, the Court simply disagrees, again, about the proof of damage. The record contained significant evidence of outages across and / or integrity corruption concerning 15-20 systems.

Multiple witnesses attributed all malicious changes only to Shahulhameed. His lawyers were effective, and did what they reasonably could, in the face of the proof. The particular file comparison about which Movant complains was not in the evidence against him. *Compare* DE #133-2, at 41-45, *with* DE #92 (Exhibit and Witness List), *and* DE #138-1, at 2-44 (Government Exhibits 5B, 5D, 5E, 5F, and 5M). Finally, the port change proof was certainly supported, but even if Shahulhameed is correct, that is only one part of the full range of evidence against him. Argument 5 is without merit.

4. Failing to properly challenge damage calculations (Argument 6)

Shahulhameed fundamentally misunderstands “damage” and “loss” within CFAA. The Court already has discussed the § 1030(e)(8) damage scope. “Loss” means “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the . . . program . . . to its condition prior to the offense.” 18 U.S.C. § 1030(e)(11). Thus, while Movant in argument focuses on losses tied to misappropriation, the statute focuses on diagnosis, remediation, and repair. Toyota rightly poured significant resources into diagnosing and fixing the problems introduced by Defendant’s post-termination conduct. Noting that the threshold is a modest \$5,000.00, the Court sees no basis for granular criticism of counsel as to this element of the crime. The case did not rise or fall on this element, as buttressed by the Sixth Circuit’s damage discussion:

Finally, the evidence shows that Shahulhameed’s conduct resulted in at least \$5,000 of damage in a one-year period. Agent Keown investigated the costs that Toyota incurred as a result of the cyberattack. Toyota provided Keown with documentation showing that Toyota employees spent 2,133 hours responding to the cyberattack between August 24 and October 30, 2012, with an estimated value of \$152,070. Toyota also paid Cincinnati Bell Technology Solutions for 200 hours of labor at \$175 per hour between August 24 and September 30, 2012, totaling \$35,000. These

figures were not challenged at trial. Contrary to Shahulhameed's argument, the prosecution demonstrated exactly how it calculated the damage that Toyota suffered. Based on this evidence, a reasonable jury could have found that Shahulhameed caused at least \$5,000 of damage.

DE #131, at 6. Simply put, none of Shahulhameed's post-hoc assessments have traction. The lawyers quite reasonably chose to focus on other elements given that Toyota undoubtedly spent exponentially more than \$5,000.00 in investigating the matter and remediating its systems after August 24, 2012. *See United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006) (upholding calculation of "loss" using hours worked and reasonable hourly rate for salaried employees' work repairing damage); *United States v. Middleton*, 231 F.3d 1207, 1214 (9th Cir. 2000) (same).

5. Failing to present evidence of change and logon time discrepancies (Arguments 7 and 9)

In arguments 7 and 9, Shahulhameed faults counsel for allegedly failing to highlight discrepancies related to the timing of particular changes to the various Toyota systems. DE #133-1, at 42-43, 46-48. Specifically, Defendant argues that particular documents not introduced at trial show that certain changes may have occurred prior to Defendant's termination from his Toyota contract and that his user login information accessed the system multiple times after that ID was supposedly terminated. *Id.* The United States responded in opposition. DE #138, at 21.

While the specific documents Shahulhameed attaches to the motion may not have been introduced at trial, defense counsel indisputably and forcefully raised these issues. During cross-examination of forensic expert Siebert, counsel confirmed that Toyota terminated Shahulhameed's network access at 6:32 a.m. on August 24, 2012. DE #127, at 46. Confirming said termination time, counsel then confronted Siebert with multiple

instances of Shahulhameed's alleged access to Toyota systems and servers at 6:33 a.m., 6:45 a.m., 6:52 a.m., 7:52 a.m., 8:02 a.m., 9:34 a.m., and 11:24 a.m. *Id.* at 67-69, 127-128. Counsel's questions elicited several questionable explanations from Siebert as to a cause of the discrepancies noted. For example, when asked about the 6:33 a.m., 6:45 a.m., and 6:52 a.m. instances of access, Siebert stated: "Well, the time – I can – the timeline that I prepared is based off just data points that were given – that we had collected. . . . So I really can't speak to the reason some of those date point show up after the fact or after that time was terminated. . . . I can only speculate as to why there's discrepancies there." *Id.* at 69. Far short of failing to elicit the timing discrepancies, defense counsel drew testimony from Toyota's IT expert that highlighted the timing issues for the jury, bringing the incongruities Shahulhameed cites in the motion to the forefront. Added documentation, largely unexplained here, would have been cumulative. The jury obviously accepted the freight of proof as incriminating against Movant. Counsel's performance utilized the strategy identified by Shahulhameed at trial. Defendant suffered no prejudice.

6. Failing to challenge certain assumption of the CBTS expert (Argument 8)

Defendant's eighth argument states, confusingly, that the "CBTS Expert explained to Jury and this Honorable Court that Ishah logged on t00tmw1d edited Siteminder configuration file without switching . . . to root Attached new evidence does show that . . . Ishah or any other user, except root user, will never be able to Modify contents, but expert Justin Hall *assumed* the command VI used to edit the files." DE #133-1, at 44 (all as in original). Counsel's failure to challenge this assumption allegedly

allowed the witness to mislead the jury. *Id.* The United States responded in opposition. DE #138, at 22.

What exactly Shahulhameed argues here is unclear. The Court perceives two interrelated complaints: (1) that counsel failed to address assumptions made by Justin Hall, a consultant hired by Toyota following the cyberattack, regarding “VI Command” and its use in editing files; and (2) that counsel did not demonstrate that changes to the “Siteminder configuration file” required root access, which Shahulhameed purportedly did not have. Per Defendant, both failures could have been resolved by the admission of a document purportedly showing that only a user with root access could have performed the Siteminder changes. *See* DE #133-2, at 48-49. Neither of these arguments is availing.

It is unclear how the attached document addresses either the “VI Command” or root access in a way relevant to the pertinent conduct. The document lists activity associated with the user account “ishah” and its access to two Toyota servers, T00TSA14 and T00TMW1D, on August 23 and 24, 2012. *Id.* T00TSA14 is the application server associated with ToyotaSupplier.com, one of the Toyota servers/websites Shahulhameed attacked on the dates in question. *See* DE #126, at 172. T00TMW1D, per the document, is associated with the Toyota Talent Management System, which was not one of the four systems at the center of the cyberattack.

For starters, nowhere does the document reference “VI Command” or any other “VI” editor program. Accordingly, the document has no relevance to *any* argument related to “VI Command,” including any supposed assumptions witness Hall made regarding said command as evidence of program edits. Further, the only reference to “root” appears in a section titled “T00TMD1_NOTES,” dated to September 15, 2011 and

linked to the Talent Management System server. DE #133-2, at 49. Shahulhameed does not demonstrate (1) how this reference supports the proposition that any required changes to the Talent Management System required root access, (2) how this root access limitation as to this secondary system (i.e. not one of the four computer systems at issue in the case) is relevant, or (3) how notation from almost a year prior the conduct at issue has any bearing on the case. A document, which contains a fleeting reference to “root,” for a tertiary server, timestamped 11 months before the cyberattack, is of questionable relevance. Shahulhameed simply cannot demonstrate prejudice resulting from counsel’s failure to introduce irrelevant evidence.

Notwithstanding the document, defense counsel certainly challenged Hall regarding the “VI Command” edit assumption and highlighted the importance of root access (and Shahulhameed’s alleged lack thereof) at various points throughout the trial. During cross-examination, Hall admitted that the “VI” command, which he had described as a “text editor . . . used for viewing and modifying files,” DE #127, at 138, did not in fact mean that any edits occurred. *Id.* at 153-54 (“Q.: Okay. Now, you were testifying about the VI.OPMN.xml, and you say that means edits were made. Is that what you’re saying? A.: No. I’m saying that that – that application can be used to edit a file. . . . Q.: Okay. So you assumed, but you have no proof whatsoever – A.: That’s correct. Q: – that any edits occurred, do you? A: That’s right. . . . Q.: It is not an edit, is it? A: That’s right.”). Counsel also established, during cross-examination of various witnesses, that (1) Shahulhameed did not have explicitly granted root access and (2) several Toyota servers required a user to have root access to make coding changes. *See, e.g.*, DE #126, at 28 (witness Cantrell testifying that Shahulhameed “was not authorized to have” root access);

id. at 30 (testifying that certain changes require root access). Again, here counsel raised, through vigorous cross-examination of Government witnesses, the very arguments Shahulhameed claims they did not. Counsel's performance with respect to these arguments, and in particular witness Hall, was in no way deficient or prejudicial.

7. Failing to investigate presence of other users on Toyota system (Argument 10)

Lastly, Shahulhameed nominally argues that counsel was ineffective for failing to investigate several other users who accessed Toyota servers at or near the time of the cyberattack. On this failure, Shahulhameed states, in its entirety:

In spite of testimony by third parties (CBTS Expert) to the fact that several other users were logged in at the time of the incident, the browser/command logs of these other users at the time of the incident were not collected and the activities at the time were analyzed based only on an **assumption**. Both Marie Barberian (have root access(i.e., keys of the kingdom)) and Devadas Veerasamy logged at 6:00 a.m. on August 24, 2012 before plug-in-cfg.xml files modified. Internet history confirms that defendant did not logged to TS.com administrative console (i.e., t00tsa14's administrative console). *See* Doc. 127, pp.161:10 – 161:17; pp. 166:24 – 167:5; pp. 171:1 – 171:7; pp. 175:10 – 175:18. When Toyota decide not to show the activity logs, the Jury and this Honorable Court and witnesses CBTS expert and FBI Agent Adam Keown were all mislead.

DE #133-1, at 49. The United States responded. DE #138, at 22-23.¹⁴

¹⁴ Defendant also makes an unsupported allegation regarding his *intent* to damage the computers at issue. DE #133-1, at 49. Specifically, he states that “insiders . . . face criminal liability only if they intend to cause damage to the computer, **not for recklessly or negligently causing damage which is defendant's case according to 1030 (g) and his duties and responsibilities** all the 18 months he was working for Toyota.” *Id.* (all as in original). Shahulhameed claims, but cites to no evidence, that any transmission of code attributable to him was merely reckless or negligent, and, therefore, not intentional. A movant must prove his case, and reliance on conclusory statements alone is inadequate. *See, e.g., O'Malley v. United States*, 285 F.2d 733, 735 (6th Cir. 1961) (“When a motion is made to vacate or set aside a judgment under Section 2255, the movant must set forth facts which entitle him to relief. Conclusions, not substantiated by allegations of fact with some probability of verity, are not sufficient to [even] warrant a hearing.”); *Ryals v. United States*, Nos. 1:05-CV-238, 1:03-CR-176, 2009 WL 595984, at *5 (E.D. Tenn. Mar. 6, 2009) (“The burden is on Ryals to articulate and plead sufficient facts to state a

For starters, although he nests this argument with the larger ineffective assistance of counsel section, Shahulhameed does not actually allege any ineffective assistance by a failure to investigate other users. The basis of his argument focuses instead on Toyota's failure to provide the activity logs of other users who accessed the relevant servers on August 23 and 24. Shahulhameed exclusively references the trial testimony of Justin Hall, a forensic investigator with third-party CBTS, to support this claim. DE #133-1, at 49; *see also* DE #127, at 161, 166-67, 171, 175. On cross-examination, Mr. Hall testified that Toyota, as part of the investigation into the cyberattack, provided CBTS with server access logs (showing which users logged into servers and when) but only provided command logs (showing what users did while logged in) for four specific accounts Toyota had identified as the source of the attack. DE #127, at 171 (“Q: Mr. Hall, can you tell me what information is contained on all the server access logs that you received? A: We were given logs showing when, which users logged into the system . . . when they — what the date and time that they logged in, and the date and time that they logged out, and the IP address on the network they came from. Q: And is it also fair — is it fair to say that the access logs doesn't [sic] tell you what the person did? A: That's right. That

claim under § 2255. . . . Because Ryals' § 2255 motion merely asserts a vague, general conclusion without sufficient substantiating allegations of fact, the motion fails to state a viable claim and is without merit.”); *United States v. Gallion*, Nos. 2:07-39-DCR-01, 2:13-7325-DCR-JGW, 2014 WL 2218361, at *14 (E.D. Ky. May 27, 2014) (“Defendant bears the burden to articulate sufficient facts to state a viable claim for relief under 28 U.S.C. § 2255. Because defendant has made only vague conclusory statements without substantiating allegations of specific facts, he has not met that burden and, consequently, he is not entitled to § 2255 relief.” (internal quotation marks and alteration removed)). Absent any competent proof, such a speculative claim does not warrant further analysis or lead to habeas relief. Further, the Sixth Circuit already determined the United States presented sufficient evidence for the jury to conclude “that Shahulhameed intentionally damaged Toyota's computer systems” based on the “destructive nature of [the] changes.” DE #131, at 5. The vast array and manual nature of various changes, as well as indicia of deception, strongly buttress the finding of mal-intent.

particular access log did not show command history. We were provided that separately.

Q: And were you provided with anything that showed you what any other persons who logged in actually did? A: Besides the four accounts that we were asked to investigate, no.”).

As to counsel’s role here, the Court notes a few things. First, the lawyers aggressively sought more information regarding the underlying Toyota record. *See* DE #127 at 161, 169. Further, they roundly criticized (in examination and argument) the quality of the investigative record, noting numerous alleged problems in document retention and the completeness of review. *See id.* at 42, 216 (noting lack of server images).

As to the overall absence of third-party scrutiny, the record shows that Toyota (and the experts, and the FBI) immediately and conclusively linked changes to a specific user and a specific laptop issuing specific commands. Via the case exhibits and case testimony, there simply is not plausible proof indicating that any other users were involved in the accesses and changes that negatively impacted Toyota. *See* DE #126 (Siebert testimony), at 232-240; Exhibits 10, 11, 12-14; DE #127 (Siebert testimony) at 107-110; *id.* (Hall testimony) at 160, 176, 188; Exhibit 3; *id.* (Keown testimony, at 202). Given that technical proof, and Shahulhameed’s compromised position and clear motives, the Court sees no basis for criticizing counsel as to this scenario. The lawyers did all they reasonably could based on the situation presented. Aiming fire at Toyota itself, which really is Shahulhameed’s thrust here, gets him no relief under § 2255.

C. *Evidentiary Hearing*

Shahulhameed requests an evidentiary hearing. DE #133, at 8. The Court must hold an evidentiary hearing unless “the files and records of the case conclusively show that the prisoner is entitled to no relief.” 28 U.S.C. § 2255(b). No hearing is necessary “where the petitioner’s allegations cannot be accepted as true because they are contradicted by the record, inherently incredible, or conclusions rather than statements of fact.” *Huff v. United States*, 734 F.3d 600, 607 (6th Cir. 2013) (quoting *Arredondo v. United States*, 178 F.3d 778, 782 (6th Cir. 1999)) (internal quotation marks removed). Shahulhameed’s claims do not warrant a hearing; the § 2255 motion filings and case record (to include all relevant transcripts and admitted exhibits) conclusively show, for the reasons stated above, that Shahulhameed’s claims fail. There are no contested factual issues that justify a hearing. The record, which needs no further development, forecloses relief.

IV. CERTIFICATE OF APPEALABILITY

A Certificate of Appealability may issue where a movant has made a “substantial showing of the denial of a constitutional right.” *See* 28 U.S.C. § 2253(c)(2). This standard requires a movant to demonstrate that “reasonable jurists would find the district court’s assessment of the constitutional claims debatable or wrong.” *Slack v. McDaniel*, 120 S. Ct. 1595, 1604 (2000); *see also Miller-El v. Cockrell*, 123 S. Ct. 1029, 1039-40 (2003) (discussing development of standard). The reviewing court must indicate which specific issues satisfy the “substantial showing” requirement. *See* 28 U.S.C. § 2253(c)(3); *Bradley v. Birkett*, 156 F. App’x 771, 774 (6th Cir. 2005) (noting requirement of “individualized assessment of . . . claims”) (citing *Porterfield v. Bell*, 258 F.3d 484, 487 (6th Cir. 2001)).

For dismissal on procedural grounds, as to when a Certificate of Appealability should issue, the movant must show that “jurists of reason would find it debatable whether the petition states a valid claim of the denial of a constitutional right and that jurists of reason would find it debatable whether the district court was correct in its procedural ruling.” *Slack*, 120 S. Ct. at 1604. Movant has not made a “substantial showing” as to any claimed denial of rights; his *Strickland* and jurisdictional claims conclusively fail. Reasonable jurists would not find the Court’s determination on the merits debatable. Accordingly, the Court recommends that the District Court entirely deny a Certificate of Appealability.¹⁵

V. RECOMMENDATION

For the reasons discussed above, the Court **RECOMMENDS** that the District Judge wholly **DENY** § 2255 relief (DE #133) and issue **NO** Certificate of Appealability.

* * * * *

The Court directs the parties to 28 U.S.C. § 636(b)(1) for appeal rights and mechanics concerning this Recommended Disposition, issued under subsection (B) of the statute. *See also* Rule 8(b), Rules Governing Section 2255 Proceedings for the United States District Courts. Within fourteen days after being served with a copy of this decision, any party may serve and file specific written objections to any or all findings or

¹⁵ The Court notes that Shahulhameed recently filed a new trial motion. DE #143. That filing has no impact on the § 2255 consideration. First, it must, by its nature, hinge on alleged “newly discovered evidence” and thus does not relate to the field of arguments critical of trial counsel’s handling of trial evidence, which Movant pursues here. Further, the motion almost certainly is untimely. The jury returned its verdict in this case on February 11, 2014. DE #95 (Verdict). Rule 33(b)(1) gave Shahulhameed only “3 years after the verdict” to file a motion premised on “newly discovered evidence.” His April 2017 filing (dated March 28, 2017), therefore, is tardy. *See United States v. Anderson*, 84 F. App’x 575, 576-77 (6th Cir. 2003) (“Anderson’s Rule 33 motion was based solely on his claim of newly discovered evidence and it was filed on December 4, 2002. This was more than three years after the April 20, 1999, guilty verdict and was thus plainly out of time.”); Rule 33, Advisory Comm. Notes, 1998 Amendments (describing amendment as “using the trial court’s verdict . . . as the triggering event”).

recommendations for determination, *de novo*, by the District Court. Failure to make a timely objection consistent with the statute and rule may, and usually does, result in waiver of further appeal to or review by the District Court and Court of Appeals. *See Thomas v. Arn*, 106 S. Ct. 466, 475 (1985); *United States v. Walters*, 638 F.2d 947, 950 (6th Cir. 1981).

This the 14th day of April, 2017.



Signed By:

Robert E. Wier

A handwritten signature in black ink that reads "REW".

United States Magistrate Judge