U.S. Department of Justice
United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

February 19, 2020

By Hand (~~CLASSIFIED SUBMISSION~~)

The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

Re: United States v. Joshua Adam Schulte, S2 17 Cr. 548 (PAC)

Dear Judge Crotty:

The Government writes in opposition to the defendant's letter motion for a mistrial (the "Mistrial Motion"), dated February 18, 2020. The Mistrial Motion is grounded in a fundamentally false premise—that the CIA suspects that someone other than the defendant "was involved in the theft and disclosure of the Vault 7 and Vault 8 information" and that the Government failed to disclose information supporting that alleged suspicion. (Mot. at 1; *see also id.* at 2 ("the CIA itself had determined that Michael was a credible suspect in the theft")). The defendant's assertions are wrong. There is only one person responsible for the theft of the CIA classified information (the "Vault 7 Information") in this case—the defendant. Neither the Government nor the CIA believes anyone else was involved, and the defendant's claims otherwise are based on a distorted reading of the CIA memorandum placing Michael on administrative leave (the "CIA Memorandum"). The CIA Memorandum explicitly states that Michael was placed on leave because of concerns he was not providing information about *the defendant* (not that he is a suspect in the theft); the Government has confirmed with the author of that memorandum that the memorandum was not intended to suggest that it was Michael rather than the defendant who stole the Vault 7 Information; and, in any event, the defendant has had all of the relevant information underlying the CIA Memorandum for months in advance of trial. Thus, there has not been any "suppression" of any relevant information—the Court has suspended Michael's cross-examination until further notice, and the defendant now not only has all of the information that was produced in discovery over the past year, but also has the CIA Memorandum itself and Michael's investigative file. Thus, there is simply no remaining purported prejudice to the defendant and the defendant's claim that the CIA Memorandum was a "bombshell" falls flat.

The defendant's other arguments for a mistrial with respect to the forensic materials—which he tries to bootstrap to the CIA Memorandum notwithstanding that the Court has already

rejected them—are equally unavailing. To start, the defendant's assertions grossly misstate the record. For example, the defendant claims that he has not had access to the March 3, 2016 Confluence backup files, but those files were produced well in advance of trial and the defendant's expert simply chose not to review them; the defendant claims that his expert was unable to show that there were other ways to access the Altabackup folders in this case, but the defendant omits that he turned down the Government's offer to permit the defendant's expert to create videos just like the one Mr. Leedom created showing how to access the backups; and the defendant contends that he was unable to replicate the Government's experts' analysis, but ignores that their opinions are based on forensic materials specifically identified to the defense months before trial. In any event, the defendant is not entitled to conduct his own investigation of the Government's files; his claims ignore controlling precedent; and the Court has already addressed this very issue on multiple occasions in the past. The defendant's motion should be denied.

Background

I. The Defendant and Michael's Relationship

The defendant and Michael worked together in the Operations Support Branch for several years together, and became friends. They socialized both at work and outside of the office. As has become abundantly clear, the atmosphere within the branch could be, at times, rambunctious, and the developers frequently joked with each other and played pranks on one another.

On one occasion, in the fall of 2015, this horseplay between Michael and the defendant got out of hand. After the two went back and forth shooting rubber bands at one another one evening, the defendant approached Michael and cornered him near a desk. Michael then struck the defendant once.

II. DEVLAN and Administrators

As the evidence at trial has demonstrated, with respect to DEVLAN, there were several different types of "administrators" on the network. Generally speaking, those types of administrators could be divided into three broad categories:

- Project-level Administrators: Employees who held administrative privileges with respect to individual projects—like Brutal Kangaroo, for example—had control over aspects of that project, such as determining who could have access to the project and what types of access they could have (*e.g.*, could the user add code to the project or merely view the project's code).

- Server Administrators: Employees who held administrative privileges with respect to certain DEVLAN servers, such as the OSB/ESXi or Stash servers, could control aspects of those servers, such as creating, deleting, or reverting virtual machines housed on those servers. In some cases, like the case of the OSB/ESXi

server at issue in the Mistrial Motion (the "ESXi Server"), employees accessed the server as an administrator by using a shared administrative account, called "root."

- [redacted] Atlassian Administrators: Employees who held Atlassian administrative privileges could control aspects of the Atlassian suite of software, which included Confluence, Stash, Jira, and Bamboo. Among other things, Atlassian administrators could use their elevated privileges to access mount points that connected the Atlassian virtual machines and servers to a space called the "Altabackups" on another server called the "NetApp" (also known as FS-01), which is also at issue in the Mistrial Motion.

Thus, while all of these employees may be referred to as "administrators," they did not all exercise control over the same parts of DEVLAN.

III. [redacted] The Events of April 15-20, 2016

[redacted] Prior to April 16, 2016, the defendant held all three types of administrative privileges described above: (i) he was an administrator of projects that he worked on, like Brutal Kangaroo and OSB Libraries; (ii) he was a server administrator for the ESXi Server and the Stash Server; and (iii) he was an Atlassian administrator. As the defendant has known since he worked at the CIA and as defense counsel has known since at least December 2018, the defendant was not the only CIA employee who held all three types of administrative privileges—Jeremy Weber, for example, also held those privileges.

[redacted] On April 15, 2016, after learning that he had been stripped of his project-level administrative privileges to OSB Libraries, the defendant confronted Mr. Weber about the change. After Mr. Weber did not accede to the defendant's request for his privileges to be restored, the defendant took the matter up with his former supervisor, Sean. After Sean also refused the defendant's request, the defendant used his administrative privileges to Atlassian to take back his project-level administrative privileges to OSB Libraries.

[redacted] On April 16, 2016, in response to the defendant's using his Atlassian administrative privileges to restore his project-level administrative privileges to OSB Libraries (despite being told explicitly that he could not retain those types of privileges), Mr. Weber, David, and Timothy—at the direction of management—restricted the number of Atlassian administrators to individuals in the Infrastructure Support Branch ("ISB"). Although that change was based on the defendant's misconduct, he was not the only one to lose his Atlassian administrative privileges at that time—all of the developers who previously had served as Atlassian administrators were stripped of these administrative privileges. As a result, these developers—including the defendant—could no longer access the Altabackups (from where the Vault 7 Information was stolen) through the mount points housed in the Atlassian virtual machines and servers.

[redacted] On the morning of April 18, 2016, the defendant met with Anthony Leonis, the then-Acting Division Chief of the Applied Engineering Division. At that meeting, Mr. Leonis provided

the defendant with a memorandum, which the defendant signed, that explicitly prohibited the defendant from trying to "attempt to restore or provide yourself with administrative rights to any project and/or system for which they have been removed." Additionally, on April 18, 2016 and then again on April 20, 2016, EDG employees, including Mr. Leonis and Mr. Weber, sent emails to, among others, all of the developers in EDG, including the defendant, that, going forward, only ISB would be administering the Atlassian programs.

[redacted] Despite these admonitions, in the evening of April 20, 2016, the defendant used the "root" account as a server administrator to log into the ESXi Server to revert the Confluence virtual machine running on that server to the version of that virtual machine that was in place on April 16, 2016. The effect of that reversion was to, among other things, restore the defendant's Atlassian administrative privileges, thus giving him the ability again to access the Altabackups. Without the privileges specifically, the defendant could not have accessed the Altabackups. While the virtual machine was in this reverted state, the defendant then accessed two specific backup files for Confluence that were created on March 3, 2016—the same data that was disclosed by WikiLeaks. After a little more than an hour, the defendant then re-reverted the Confluence virtual machine back to its April 20, 2016 state, deleting the records of his conduct. To further cover his tracks, the defendant then also logged into the ESXi Server through a second means—his SSH key (which was the only SSH key stored on that server)—and proceeded to systematically delete log files that recorded his conduct (such as, for example, log files that would have recorded a command to "copy" the stolen data).

[redacted] The evidence introduced at trial proves conclusively that it was the defendant who, on April 20, 2016, logged into the ESXi server as a "root" administrator, reverted the Confluence virtual machine to its April 16, 2016 state, and then proceeded to delete the log files of his activity while the system was in its reverted state. That evidence includes, for example, log files from the defendant's DEVLAN workstation that show that (i) the defendant created an April 20 snapshot before reverting the Confluence virtual machine (*see* GX 1202-7); (ii) the defendant then reverted the Confluence virtual machine back to its April 16 state (*see* GX 1202-18); (iii) the defendant then reversed the reversion and took the system back to its April 20 state (*see* GX 1202-19); (iv) the defendant then deleted the April 20 snapshot that he created (*see* GX 1202-21); and (v) the defendant then deleted the log files on the ESXi server that would have shown his conduct during the reversion (*see* GX 1203-8, 29, 55, 56, 60, & 63). All of these files were found on the defendant's DEVLAN workstation, a fact that the defendant not only did not challenge, but indeed to which he stipulated. (*See* GX 3005 at ¶ 1 (agreeing that GX 1202-7, 1202-18, 1202-19, 1202-21, 1203-8, 1203-29, 1203-55, 1203-56, 1203-60, and 1203-63 were all files found on components of the defendant's DEVLAN workstation)). The evidence also demonstrated that while the Confluence virtual machine was reverted to its April 16 state—when the defendant had the administrative privileges necessary to access the Altabackups—the March 3 Confluence backup files "date accessed" time was modified, a computer action that is consistent with copying those files. (*See* GX 1207-27 & 30). The evidence also showed that the Confluence data included in the Vault 7 Information came from those backup files. (Tr. 1364-1366 (testimony of Michael Berger)).

[redacted] At the time of the reversion, Michael was working in a different part of the building. After the defendant began the reversion and accessed the March 3 backup, he sent an electronic message to Michael over their unclassified (*i.e.*, non-DEVLAN) system, asking whether Michael wanted to go to the gym, an activity they commonly did together. Michael promptly responded, asking the defendant when he wanted to go, but the defendant did not respond at that time. Approximately 45 minutes later, Michael again asked over the unclassified system when the defendant wanted to go to the gym, and again received no response. Michael then sent an electronic message to the defendant over DEVLAN at 6:35 pm—the defendant responded within two minutes to this message, asking if they could meet in 15 minutes.

[redacted] While Michael was waiting for the defendant, Michael noticed activity on the DEVLAN system that he felt was strange and took a screenshot (the "Screenshot") of his computer screen to capture that activity at 6:56 pm, just after the defendant accessed the March 3, 2016 Confluence backup files and had then reverted the Confluence virtual machine back to its April 20 (*i.e.*, current state). In particular, Michael was struck by the lack of any log files displayed on the screen where he would have expected to see them. Michael was concerned that the defendant may have engaged in inappropriate behavior, and tried to determine what had happened to the system. Michael ultimately concluded, however, that the reason he could not view any log files may have been because he was logged in using his regular user account, as opposed to the "root" account. He also eventually came to believe that—because Mr. Weber had said that the Atlassian administrator privileges were going to be restricted—the defendant should not have had the necessary privileges to revert the system. Michael then went to the gym with the defendant, and the two then later left the Center for Cyber Intelligence office (the "CCI Office") at the same time. Michael did not discuss with the defendant or Mr. Weber the activity he saw on DEVLAN that night nor did he inform anyone that he had taken the Screenshot.

IV. [redacted] The FBI Interviews of Michael

[redacted] After WikiLeaks began to disclose the Vault 7 Information, the Federal Bureau of Investigation ("FBI") began an investigation into the leak. That investigation included, among other things, interviewing everyone with access to DEVLAN. The investigation also included seizing and reviewing an unprecedented amount of forensic material from the CCI Office and CCI's foreign offices.

[redacted] During the course of the investigation, the FBI, together with prosecutors from this Office, interviewed Michael on March 16, 2017, June 1, 2017, June 2, 2017, June 6, 2017, August 30, 2017, March 8, 2018, August 16, 2019, and January 13, 2020 (collectively, the "Michael Interviews"). In his initial March 16 interview, Michael stated, in substance and in part, that Michael had not observed any "remarkable changes" in the defendant's behavior during the time Michael had known him. That observation was at odds with the descriptions of the defendant's behavior from other witnesses, who had described how the defendant became angry after Mr. Weber had revoked his administrator privileges to OSB Libraries.

[redacted] During his first four interviews, Michael also did not disclose the fact that he had taken the Screenshot to the FBI. After the FBI found the Screenshot in Michael's home folder on the NetApp Server, FBI agents confronted Michael with it during the August 30 interview. During the interview, Michael stated that he remembered taking the Screenshot to document strange activity on the system. At the conclusion of the interview, one of the agents asked Michael if he would be willing to take a polygraph examination, which Michael declined to do. As the report of the interview indicates, Michael stated that he was concerned about taking a polygraph [redacted] Michael also expressed concern that the agent's request that Michael take a polygraph suggested that Michael was now a subject of the investigation. The FBI did not interview Michael again until March 8, 2018.

[redacted] On August 16, 2019, the FBI and two members of the Government's trial team interviewed Michael in New York. As the notes of that meeting reflect, the FBI and the prosecutors reminded Michael about the potential criminal penalties that could result if he was not honest with law enforcement, told him that the Department of Justice had no control over the CIA's employment decisions, and advised Michael that he could have an attorney present if he wished. At the prosecutors and the FBI's request, Michael then described again the events of April 20, 2016. When asked why he had not disclosed the Screenshot to the FBI earlier, Michael stated that he had not remembered taking the Screenshot until the FBI showed the document to him. The interview then ended when Michael indicated that he wanted an attorney.

[redacted] Michael ultimately retained an attorney, who contacted the prosecutors and indicated that Michael wished to speak with them again. The prosecutors and the FBI met with Michael and his attorney on January 13, 2020. After meeting with Michael and his attorney, the Government decided that it would call Michael as a witness at trial, and began to meet with him to prepare for trial.

V. [redacted] The CIA Placed Michael on Administrative Leave

[redacted] On August 16, 2019, after learning about his interview earlier that day, the CIA decided to place Michael on paid administrative leave. That day, an employee with the Agency's Counterintelligence Mission Center ("CIMC") submitted the CIA Memorandum seeking approval for the action. The CIA Memorandum, in a section entitled "Justification," states that "[Michael's] lack of cooperation with inquiries into his past activities with the primary person of interest in the FBI investigation and his unexplained activities on the computer system from which the [Vault 7 Information was stolen], and raises significant concern about his truthfulness, trustworthiness, and willingness to cooperate with both routine OS reinvestigation processes and the criminal investigation into the left from his office." CIA Memorandum at 1. The author goes onto write in that section "CIMC believes curtailing [Michael's] access to CIA spaces and data systems is necessary to safeguard against potential future losses of sensitive and classified information." *Id.* Nothing in the CIA Memorandum—whether in the "Justification" section or elsewhere—states that the CIA viewed Michael as a potential suspect in the theft of the Vault 7

Information, rather than simply an employee who was uncooperative with an investigation into the defendant.

[redacted] The CIA Memorandum also provides background for the administrative leave request. For example, the memorandum discusses how Michael had not been cooperative with an internal CIA investigation into Michael's physical altercation with the defendant. *See* CIA Memorandum at 2. [redacted] The CIA Memorandum also describes several "concerns" with Michael, "including his close proximity to the theft of the data and his relationship with Joshua Schulte, the individual charged with the theft of the data." *Id.* at 3. The memorandum further stated that "[f]orensic analysis of [Michael's] activity on the DEVLAN suggests that [Michael] may have additional knowledge of anomalies on the system at the time of the theft." *Id.* Based on these concerns, the memorandum described a "Risk Assessment" that CIMC viewed Michael's "lack of cooperation as a significant and untenable risk to the security of the operations on which he now works and any new tools he deploys for CCI." *Id.*

[redacted] On August 19, 2019, Michael was notified that he was being placed on paid administrative leave. He was not given a copy of the CIA Memorandum or provided with information as to why he was being placed on leave.

VI. [redacted] FBI Reporting about Michael's Administrative Privileges

[redacted] Michael's "system administrator" privileges were well-documented in the reports of the FBI interviews. Indeed, Michael's "system administrator privileges" were discussed in at least three different interviews, one of Michael and the other two of Mr. Weber:

- [redacted] In a March 22, 2017 interview, Weber stated that "*Michael, [the defendant], [Weber], and [Matt] had administrative access to the ESXi server* . . . . A root password was required to directly log into the ESXi server and this password was shared on OSB's Confluence page that all of OSB had access to." CLASSIFIED JAS_001318 – 001320 (emphasis added).

- [redacted] In a May 26, 2017 interview, Weber stated that he "believed that [Matt] and [Michael] were possibly added as [ESXi] administrators later." CLASSIFIED JAS_010153 – 010159.

- [redacted] In a March 8, 2018 interview, Michael explained the relevant distinction in administrative privileges: "There is a difference between being considered an Atlassian administrator and having the root password for the ESXi server. The root password for the ESXi server was likely needed to create and control VMs, which are frequently used by developers for testing. *[Michael] believed he used the ESXi root password to create VMs*. The status of being an Atlassian administrator is reflected in the user's domain credentials. [Michael] is not

aware of how to get access to Atlassian as an administrator." CLASSIFIED JAS_010514 (emphasis added).

[redacted] These reports make clear that Michael never had Atlassian administrator privileges, and thus did not have the ability to access or copy the Altabackups (from which the Vault 7 Information was stolen).

VII. [redacted] The Discovery Process

[redacted] The Government charged the defendant with crimes related to the Vault 7 Information in June 2018, and began to produce discovery specific to those charges shortly thereafter. By December 10, 2018, the Government had produced to the defense, among other things:

- All of the FBI reports of witness interviews (the "302s") that had been conducted to date, including all of the 302s of the interviews with Michael and Mr. Weber.
- Log files from the three hard drives and virtual machine that made up the defendant's CIA workstation (the "Schulte Workstation").
- Log files from the ESXi Server.
- Two Confluence databases that included the March 3, 2016 and March 4, 2016 Confluence backups (*i.e.*, the backup that was stolen and the one immediately after it).
- Files from the defendant's home folder on the NetApp Server, including the computer scripts that ran daily to create the backups in the Altabackups.
- The Screenshot taken by Michael.
- Login attempts into the Confluence virtual machine.
- Audit logs for OSB Libraries and Brutal Kangaroo showing the April and May 2016 changes in administrator privileges.
- Files from the NetApp Server showing the users of DEVLAN.
- Database queries showing the Atlassian administrators (which show that Michael was not an Atlassian administrator and thus did not have access to the Altabackups).
- Network diagrams describing the structure of the system.

- Screenshots showing the Confluence backups stored on the Altabackups as of April 2016 (the "Altabackups Screenshots").

- The forensic image of the thumb drive that was plugged into the Schulte Workstation on April 20, 2016, and then repurposed on April 21, 2016.

[redacted] The Government did not produce the full "mirror images" of the ESXi Server, the NetApp Server, or the Schulte Workstation to the defense. Instead, the Government moved pursuant to Section 4 of the Classified Information Procedures Act ("CIPA") to withhold those images from the defendant on the ground that these images contained classified information that was not discoverable, and even if so, not relevant or helpful to the defense, as required under the law. *See United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008). Over the next several months, the Court conducted several *ex parte* hearings and accepted submissions from both the Government and the defense concerning the Government's Section 4 motion. On July 22, 2019, the Court granted the Government's Section 4 motion in part, but directed the Government to produce specific documents to the defense (one of which has now been entered as an exhibit at trial). CIPA Section 4 Order at 7-8. In granting the Government's motion, the Court noted that "granting [the defendant] unfettered access to the Schulte Workstation and DEVLAN would gut the entire rationale of CIPA" and that the defendant was not "entitled to unfettered access" to these CIA computer systems. *See id.* at 11-12. The Court stated, however, that the defendant could still submit a "more tailored request" and indicated that it would be helpful if the defendant "would communicate his thinking of how others are responsible for the theft." *See id.* at 12.

[redacted] Over the next several months through the start of trial, the defendant continued to object to his lack of access to the full "mirror images" of the ESXi Server and other forensic items, and even, the Government understands, submitted an *ex parte* declaration from the defense's expert trying to explain why the defense needed to be able to review the entire ESXi Server. At the same time, when the defendant did actually submit more tailored requests, the Government responded to them. Thus, for example, on June 14, 2019, the Government produced, among other things:

- Additional portions of the ESXi Server, including unallocated space.

- Log files from the workstations of the employees besides the defendant who had Atlassian administrator privileges (the privileges used to access the Altabackups) during the relevant time period (which, like the log files from the Schulte Workstation, would show activity on the workstation).

- Registry information (which would show, for example, if removable media had been plugged in or out of the computer) for these same employees' workstations.

- All available application logs for the Confluence virtual machine from April 7, 2016 through April 25, 2016 (*i.e.*, other than what Schulte erased).

On August 16, 2019, the Government also identified to the defense the portions of the forensic discovery that, at that point, the Government intended to rely upon at trial.

On November 5, 2019, in response to a defense request specifically made in connection with the timing analysis conducted by Michael Berger, the Government and the CIA arranged for a standalone laptop (the "Standalone") to be made available in CIA space for review by defense counsel and the defense expert. The Standalone was loaded with (i) the most recent Stash backup available to the Government; (ii) Stash repositories for all of the tools that WikiLeaks disclosed (*i.e.*, the information against which one could compare the disclosed material to determine the date of the disclosed data); (iii) the March 2 and 3, 2016 Confluence backup files and all of the Confluence data points used by Mr. Berger to conduct his timing analysis; and (iv) the same Crowd databases against which Mr. Berger ran queries to generate the information about administrative privileges to which he testified.[1] Before examining the materials on the Standalone, the defendant complained that they were insufficient and that he should receive the entirety of EDG's Stash and Confluence holdings. The defense expert briefly examined the Standalone in December 2019 and informed the CIA that he would need to conduct more research and to schedule another session. The defense did not raise any issues with the Atlassian backups provided on the Standalone or make any more tailored requests, but simply insisted to the Court that as a blanket matter, the Government's production was insufficient.

On January 13, 2020, the defense filed a letter with the Court in which it stated that the defense wanted, among other things, "access times" for the Altabackups Screenshots. On January 28, 2020, the Government produced the updated version of the files that included the access times, and which showed that the March 3, 2016 Confluence backup files were accessed during the defendant's reversion, which confirmed the Government's theory of prosecution. Despite the fact that the Government produced the new Altabackups Screenshots before trial, marked some of them as Government exhibits GX 1207-27 and 1207-30, included these exhibits in both Mr. Leedom's and Mr. Berger's demonstrative exhibits that were produced to the defendant prior to these witnesses' testimony, and in fact admitted GX 1207-27 and 1207-30 into evidence pursuant to a stipulation, the defendant did not object until the Mistrial Motion, nearly two weeks into trial.

VIII. Defense Counsel's Cross-Examination of Michael

On February 11, 2020, the Government notified the defense that Michael had been placed on paid administrative leave based on "security concerns based on the CIA's assessment that he did not fully cooperate with the investigation into the leaks," and that, as a result, the U.S.

---

[1] The Government had already produced the March 3 and March 4, 2016 Confluence backup files on December 10, 2018. The Government reproduced the March 3, 2016 backup files on the Standalone out of an abundance of caution to ensure that the defendant had access to all of the relevant information underlying Mr. Berger's timing analysis. Thus, through the course of this case, the defendant has been provided with three different Confluence backup files—those dated March 2, 2016 (the day before the stolen backup files); March 3, 2016 (the stolen backup files); and March 4, 2016 (the day after the stolen backup files).

Attorney's Office was paying for his travel expenses, unlike the other CIA witnesses. The following day, Michael began to testify. Defense counsel also began to cross-examine the witness, and was still cross-examining the witness at the close of the trial day. At the end of the trial day, defense counsel sought production of the CIA Memorandum, and the Court directed the Government to provide it to the Court for *in camera* review. The Government submitted the memorandum to the Court later that day.

[redacted] The following morning, before cross-examination, the Court directed the Government to produce the CIA Memorandum to the defense. That morning, while defense counsel continued her examination, the Government gave the memorandum to defense counsel. During the cross-examination, defense counsel questioned Michael extensively about his interviews with the FBI using the 302s. At one point, defense counsel used the 302 of Michael's August 30, 2017 interview to question the witness about the Screenshot and the fact that he had not told the FBI about it. (*See* Tr. at 1298-1300). Similarly, she asked the witness about the FBI's request that he take a polygraph examination at the conclusion of that interview, and his refusal to undergo the testing. (*See id.* at 1309). During cross-examination, defense counsel also introduced into evidence, without objection from the Government, a screenshot demonstrating that Michael had some access to the defendant's virtual machine. (*See id.* at 1275). Finally, defense counsel also began to question Michael about the circumstances of his placement on administrative leave, even eliciting that, in the wake of it, Michael had retained a well-known criminal defense attorney who was experienced in representing clients charged with illegally disclosing classified information. (*See id.* at 1317-18).

[redacted] During a break in the examination, defense counsel informed the Government that they had a matter to take up with the Court *ex parte* about the CIA Memorandum. Defense counsel then met with the Court. At the conclusion of that meeting, defense counsel made an application to suspend the balance of the cross-examination. The Court determined that the Government should have produced the CIA Memorandum to defense earlier, and granted the defense's application.

[redacted] Over the weekend between the suspension of Michael's testimony and the resumption of trial, the Government took steps to confirm that—except for the fact of the paid administrative leave—the information upon which CIMC's statements in the CIA Memorandum were based had previously been produced to defense counsel. First, the Government spoke with the author of the CIA Memorandum, who confirmed that the concerns described in the memorandum referred to (1) Michael's communications with the defendant during the reversion period; (2) Michael's taking of the Screenshot (which is the "forensic activity" described in the memorandum); (3) Michael and the defendant leaving together that evening; and (4) the CIA's perspective that Michael had not been cooperative with the investigation into the defendant or into the CIA's internal investigation into Michael's altercation with the defendant. Second, the Government reviewed Michael's CIA security file and the investigative file prepared by CIMC. The review confirmed that there was no additional information to be disclosed to the defendant

[redacted]

[redacted] Third, the Government re-reviewed the produced 302s to ensure that the defense had previously been provided with the information about Michael's administrative privileges. The Government submitted a letter to the Court on February 18, 2020, outlining the steps it had taken.

[redacted] That same morning, the defendant submitted the Mistrial Motion, seeking a mistrial based on the timing of the disclosure of the CIA Memorandum and a renewed complaint that the Government did not produce full "mirror images" of the ESXi Server or the NetApp Server.

[redacted] ARGUMENT

[redacted] The defendant's Mistrial Motion requests severely disproportionate relief, is based on a twisted and misleading reading of the CIA Memorandum, ignores the information that has previously been produced to the defense. Moreover, the defense's argument that Mr. Leedom's testimony has opened the door to revisiting the Court's Section 4 ruling that the Government could withhold complete forensic images of the ESXi Server and the NetApp Server takes one of Mr. Leedom's answers completely out of context and asks the Court to not only ignore the balance of his testimony, but also all of the information that has already been provided to the defense. Therefore, the Mistrial Motion should be denied.

I. [redacted] Applicable Law

[redacted] "A defendant's motion for a mistrial may be granted where something has occurred to interfere with the defendant's right to a fair trial." *United States v. Yannai*, 791 F.3d 226, 242 (2d Cir. 2015). The decision whether to declare a mistrial "is left to the sound discretion of the [trial] judge." *Renico v. Lett*, 559 U.S. 766, 774 (2010) (internal quotation marks omitted). A mistrial, however, is a "drastic remedy." *United States v. LaFroscia*, 485 F.2d 457, 458 (2d Cir. 1973). A court's power to grant a mistrial should only be used "with the greatest caution, under urgent circumstances, and for very plain and obvious causes." *Renico*, 559 U.S. at 774 (internal quotation and citation omitted); *United States v. Klein*, 582 F.2d 186, 190 (2d Cir. 1978) (quoting *United States v. Perez*, 22 U.S. 579, 580 (1824)).

[redacted] The Government's discovery obligations in criminal cases begin with Federal Rule of Criminal Procedure 16(a)(1)(E), which provides, in pertinent part, that the Government must disclose to the defense documents and objects that are "within the government's possession, custody, or control" if they are "material to preparing the defense" or will be used by the Government in its case-in-chief at trial. Evidence is material to the defense "if it could be used to counter the government's case or to bolster a defense," but "information not meeting either of those criteria is not to be deemed material within the meaning of" Rule 16. *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (interpreting the Rule's predecessor, Fed. R. Crim. P. 16(a)(1)(C)). "Materiality means more than that the evidence in question bears some abstract logical relationship to the issues in the case. There must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991) (internal

quotation marks omitted). In addition, with respect to the Government's obligations to disclose materials related to its experts, Federal Rule of Criminal Procedure 16(a)(1)(G) requires that the Government must disclose a "written summary of any testimony that the Government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial" and that the summary describe "the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications." Federal Rule of Evidence 705 permits an expert to "state an opinion—and give the reasons for it—without first testifying to the underlying facts or data" but also states that "the expert may be required to disclose those facts or data on cross examination."

[redacted] Of course, the Government also has an obligation under the Due Process Clause to disclose to the defendant material exculpatory and impeaching evidence. *See Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972). To warrant a new trial based on a violation of this obligation, "a defendant must show that: (1) the Government, either willfully or inadvertently, suppressed evidence; (2) the evidence at issue is favorable to the defendant; and (3) the failure to disclose this evidence resulted in prejudice." *United States v. Coppa*, 267 F.3d 132, 140 (2d Cir. 2001). Thus, it is not enough to show that the Government failed to turn over favorable evidence. A *Brady* or *Giglio* violation will result in a new trial only "if the undisclosed information is 'material,' within the exacting standard of materiality established by the governing case law." *United States v. Spinelli*, 551 F.3d 159, 164 (2d Cir. 2008); *accord United States* v. *Rivas*, 377 F.3d 195, 199 (2d Cir. 2004); *United States v. Middlemiss*, 217 F.3d 112, 123 (2d Cir. 2000).

[redacted] "There is no general constitutional right to discovery in a criminal case, and *Brady* did not create one." *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977); *see also United States v. Polowichak*, 783 F.2d 410, 414 (4th Cir. 1986) ("*Brady* did not create a criminal right analogous to discovery in a civil case."); *United States v. Evanchik*, 413 F.2d 950, 953 (2d Cir. 1969) ("Neither [*Brady*] nor any other case requires the government to afford a criminal defendant a general right of discovery."). Nor does the defendant have a "constitutional right to conduct his own search of the [Government's] files to argue relevance." *Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987). "Unlike Rule 16 and the Jencks Act . . . *Brady* is not a discovery rule, but a rule of fairness and minimum prosecutorial obligation . . . ." *Maniktala*, 934 F.2d at 28 (internal quotation marks omitted)). It is the prosecution team's duty to evaluate whether exculpatory information existed within its holdings. *See United States v. Agurs*, 427 U.S. 97, 109 (1976) ("If everything that might influence a jury must be disclosed, the only way a prosecutor could discharge his constitutional duty would be to allow complete discovery of his files as a matter of routine practice. . . . [T]he Constitution surely does not demand that much.").

[redacted] Where a new trial is sought based on a proffered *Brady* violation, the Supreme Court has said that the "touchstone of materiality is a reasonable probability of a different result," that is, whether "the government's evidentiary suppression undermines confidence in the outcome of the trial." *Kyles v. Whitley*, 514 U.S. 419, 434 (1995) (internal quotation marks omitted); *accord United States v. Bagley*, 473 U.S. 667, 682 (1985) (suppressed evidence is "material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different"); *Strickler v. Greene*, 527 U.S. 263, 281 (1999) ("[T]here is never a real '*Brady* violation' unless the nondisclosure was so serious that there is a reasonable

probability that the suppressed evidence would have produced a different verdict."); *United States v. Douglas*, 525 F.3d 225, 244-45 (2d Cir. 2008); *United States v. Payne*, 63 F.3d 1200, 1209 (2d Cir. 1995) ("[U]ndisclosed evidence will be deemed material only if it 'could reasonably be taken to put the whole case in such a different light as to undermine confidence in the verdict."' (quoting *Whitley*, 514 U.S. at 435)).

[redacted] Moreover, "evidence is not considered to have been suppressed within the meaning of the *Brady* doctrine if the defendant or his attorney either knew, or should have known, of the essential facts permitting him to take advantage of that evidence." *United States v. Paulino*, 445 F.3d 211, 225 (2d Cir. 2006) (internal quotation marks omitted). There can be no "suppression" for *Brady* purposes when the defense actually possessed the information in time for effective use at trial or to otherwise investigate the information, even if the evidence was produced after trial had begun. *See Coppa*, 267 F.3d at 144 ("[A]s long as a defendant possesses *Brady* evidence in time for its effective use, the government has not deprived the defendant of due process of law simply because it did not produce the evidence sooner.").

II. [redacted] Discussion

[redacted] None of the bases offered by the defendant support granting the "drastic" remedy of a mistrial, or, indeed, any relief more than what the Court has already afforded the defense. With respect to Michael and the CIA Memorandum, the defense cannot establish materiality or suppression because they had all of the underlying information before cross examination started and they now have the memorandum itself to pursue whatever questioning they want when cross examination resumes. Moreover, the defense has had all of the information necessary to make "major strategic trial decisions" about "whether, and how aggressively to blame Michael for the theft and disclosure of the [Vault 7 Information]," Mistrial Motion at 6, for several months, and in most cases, more than a year. Indeed, defense counsel already laid the groundwork for precisely that (ultimately meritless) argument. The CIA Memorandum does not change that calculus because the memorandum categorically does not say that the CIA viewed Michael as a potential perpetrator of the theft and disclosure. The only information that the CIA Memorandum added to the information already available to the defense was that the CIA questioned Michael's credibility, and that type of opinion evidence is inadmissible as a matter of law.

[redacted] Further, with respect to Mr. Leedom's testimony and the Government's production of forensic material, the defense has had all of the information upon which Mr. Leedom relied to arrive at his opinions well before trial, and thus a reasonable opportunity to test and scrutinize those opinions. To argue to the contrary, the defendant twists one of Mr. Leedom's answers and mischaracterizes the Government's discovery productions. The same goes for Mr. Berger—while the defense complains that it did not have access to the files underlying his opinions, the truth of the matter is that all of that information was provided to the defense well before trial. Therefore, the Court should deny the Mistrial Motion.

A. [redacted] The CIA Memorandum and Michael's Administrative Leave Are Not Grounds for A Mistrial

[redacted] The defense claims that had they had the CIA Memorandum earlier they would have been able to develop an argument that it was Michael, not the defendant, who stole the Vault 7 Information. To the extent that memorandum refers to supposed suspicious activity by Michael during April 2016, the underlying evidence of that activity was provided to the defendant long before trial. For example, the CIA Memorandum describes that Michael was at work during the reversion and left the building with the defendant that night. But the defendant has had badge records for Michael demonstrating that fact since at least September 30, 2019. Moreover, those records affirmatively undercut the defendant's argument, because they show that Michael did not enter the vault on the eighth floor in which the defendant's DEVLAN workstation was located during the reversion and, in fact, was on a floor of the building during much of reversion that was not even part of EDG's space. (*Compare* GX 105 (the defendant's badge records) & 115 (Michael's badge records)). The CIA Memorandum further recounts that Michael was in communication with the defendant during the reversion period—but those communications were included in discovery that the defendant has had at least months before trial, such as the defendant's SameTime communications with Michael (*see* GX 719) and the defendant's DEVLAN IRC chats with Michael (*see* GX 726). And again, these records are harmful, not helpful, to the defendant because they show that around the time of the reversion, he was logged into and sitting at his DEVLAN workstation (*see also* GX 1070 (April 20, 2016 email from the defendant to Anthony Leonis sent during the reversion)). Finally, the CIA Memorandum describes Michael's "forensic activity" on DEVLAN at the time, which, as the Government has already confirmed to the Court and defense counsel, is a reference to the Screenshot that he took that showed the absence of log files on the system on April 20, 2016, which the defendant has had since December 10, 2018. There is no "suppression" of any of this information—it was all provided to the defense in discovery long before trial.

[redacted] Defense counsel's cross examination of Michael makes clear that the strategic decision to accuse Michael as a potential alternative perpetrator (however implausible) was an option that the defendant seems to intend to pursue. Defense counsel questioned Michael about the Screenshot and what it showed. (*See* Tr. at 1299). She cross-examined Michael about the fact that he did not initially disclose the Screenshot to the FBI, and instead only discussed it when it was shown to him by the agents. (*See id.* at 1300). Defense counsel even introduced a screenshot showing that Michael had an account on the defendant's virtual machine, which the defense had since December 10, 2018. (*See id.* at 1275). Thus, to the extent the defendant wants to develop through cross examination or otherwise an argument that it was Michael, and not the defendant, who was responsible for the theft and disclosure of the Vault 7 Information, he already started that process and can continue when cross examination resumes. *See Coppa*, 267 F.3d at 144 ("[A]s long as a defendant possesses *Brady* evidence in time for its effective use, the government has not deprived the defendant of due process of law simply because it did not produce the evidence sooner.").

[redacted] The only "new" information provided to the defendant in the CIA Memorandum is the fact that the CIA placed Michael on administrative leave in August 2019 and questioned his credibility. But critically, as the memorandum itself makes clear, the CIA did not take this action out of any belief that Michael stole the Vault 7 Information. Instead, as the memorandum states, the CIA disciplined Michael because of a perceived "lack of cooperation with inquiries into past activities with the primary person of interest in the FBI investigation [*i.e.*, the defendant] and his unexplained activities on [DEVLAN]." CIA Memorandum at 1. In other words, the CIA's principal concern was that Michael did not fully disclose information beginning in 2017 about what he did with the defendant, and the Screenshot. As the CIA Memorandum itself makes clear, in light of the release of Vault 7 and the security issues exposed by the leak to the defendant's conduct, the CIA viewed it as an unacceptable risk *in August 2019* to have an employee who may be unhappy with the Agency and not forthcoming during the investigation to continue to have access to the sensitive information on the CIA's systems. *See* CIA Memorandum at 3 ("CIMC views [Michael's] lack of cooperation as a significant and untenable risk to the security of *operations on which he now works and any new tools he deploys for CCI*") (emphasis added). That, in the CIA's view, Michael had developed into a potential risk years after the disclosure of the Vault 7 Information is simply not probative of an alternative perpetrator theory regarding the theft and disclosure of the Vault 7 Information years before. And even reading the memorandum's reference to "unexplained activity on [DEVLAN]" to mean something more than Michael's taking of the Screenshot (which is all that the language refers to), an opinion that an individual may be complicit in a crime is not competent evidence. *See United States v. Garcia*, 413 F.3d 201, 215 (2d Cir. 2005) (precluding testimony by law enforcement agent "that, in his opinion, . . . defendant was a culpable member of the charged conspiracy" because "a 'lay opinion' as to a person's culpable role in a charged crime . . . is not presenting the jury with the unique insights of an eyewitness's personal perceptions"). Thus, the CIA's leave decision as reflected in the CIA Memorandum adds no force to the defendant's already feeble alternative perpetrator theory regarding Michael, defense counsel has already demonstrated during cross examination of Michael thus far that she has adequate information to pursue that theory and there is no prejudice because she can continue to pursue it when cross examination resumes.

[redacted] Finally, even disclosure of the CIA's views about Michael's credibility do not support a mistrial. Initially, a CIA employee's view of Michael's credibility is not admissible at trial. In general, testimony regarding the credibility of other trial witnesses is impermissible. *United States v. Aquart*, 912 F.3d 1, 34 (2d Cir. 2018). "As a matter of law, the credibility of witnesses is exclusively for the determination by the jury, and witnesses may not opine as to the credibility of the testimony of other witnesses at the trial." *United States v. Truman*, 688 F.3d 129, 143 (2d Cir. 2012) (quoting *United States v. Forrester*, 60 F.3d 52, 63 (2d Cir. 1995)). Thus, the statements about Michael's credibility in the CIA Memorandum cannot create "a reasonable probability that the suppressed evidence would have produced a different verdict," *Strickler*, 527 U.S. at 281, because the defendant could not have offered them as evidence at trial. Moreover, as the CIA Memorandum states, the CIA's credibility concerns are based on Michael's responses to questioning by the FBI during its interviews and Michael's refusal to discuss the circumstances of his altercation with the defendant during an internal CIA interview. The defendant had all of the information necessary to pursue that line of cross-examination—he had all of the reports of

Michael's interview with the FBI (which included the agents confronting him with the Screenshot, his refusal to take a polygraph when asked by the agents, and the August 16, 2019 notes of the interview that led to Michael's administrative leave status and retention of an attorney) and the CIA interview in which he refused to answer questions about the fight.

[redacted] In sum, Michael's administrative leave based on the Agency's security concerns caused by its perception of his candor was produced to the defense before Michael took the stand. The bases for those concerns were produced to the defense long before trial in discovery. Whatever information the defendant needed to make the strategic decision of how to approach Michael and his testimony were in the defense's possession with more than enough time for him to make those decisions and he may use those materials when cross examination continues. Therefore, the Mistrial Motion should be denied.

B. [redacted] A Mistrial Is Not Warranted Based on the Withholding of the Full Forensic Images of the ESXi and NetApp Servers

[redacted] The defendant's attempt to rehash the Court's prior discovery rulings with respect to the images of the ESXi and NetApp Servers as a basis for a mistrial fare no better. None of the defendant's laundry list of complaints is accurate, and instead rely on a mischaracterization of the record.

[redacted] *First*, with respect to Mr. Leedom's testimony, none of the opinions to which he testified relied on any information from the images of the ESXi and NetApp Servers beyond what was produced to the defense. Indeed, starting in July 2019, the Government began to identify the specific forensic artifacts underlying Mr. Leedom's opinions. The parties discussed these forensic artifacts extensively during CIPA proceedings in November and December 2019, well in advance of trial. Moreover, the Government produced a detailed expert notice to the defense on October 18, 2019 (and that notice specificially stated that Mr. Leedom's opinions were based on the forensic materials produced in discovery to the defendant), and began producing drafts of Mr. Leedom's trial presentation weeks before trial. The defense raises 10 purported areas by which they were prejudiced by the Government's alleged withholding of forensic material, none of which is accurate:

1. [redacted] The defense claims that it could not do the same analysis as the Government of the "damage" to the March 3, 2016 Confluence backup files. *See* Mistrial Motion at 9. The defense is wrong. Initially, Mr. Leedom testified that the "damage" to that backup file was the result of an error in the computer script that was used to create not only the March 3, 2016 backup files, but all of the backup files in the Altabackups. (*See* Tr. at 1117-1119). That script was produced to the defendant on December 10, 2018, meaning that the defendant had more than enough time to examine it to determine whether Mr. Leedom's opinion about the error was accurate. Moreover, the defense had access the March 3, 2016 backup files because the Government produced them, first on December 10, 2018 (which the defense confirmed in a September 26, 2019 letter to the Government and did not raise any

issues with the Government's production of those files), and then again on the Standalone in November 2019. The defendant's claim that he needed access to a mirror image of the NetApp server to review complete files from that server is a non-sequitur, because the defendant has had access to the specific files at issue.

2. [redacted] The defense claims that they could not examine "vi-client logs" the way that the Government could. *See* Mistrial Motion at 10. To be sure, the Government did not produce the "vi-client logs" for the hundreds of DEVLAN workstations that the FBI reviewed during the investigation, because the Government was also not obligated to do so. The Government is aware of its *Brady* obligations with respect to these materials and is in compliance with them. Mr. Leedom did not testify about those logs and the Government has not relied on those logs in its case-in-chief, and so Rule 16 does not obligate the Government to produce them. Contrary to the defendant's repeated suggestion, in any criminal case, the defendant does not have a "constitutional right to conduct his own search of the [Government's] files to argue relevance." *Ritchie*, 480 U.S. at 59. That is particularly inappropriate in a case such as this one in which, to accomplish what the defendant claims is necessary, the Government would have to indiscriminately turn over classified information to the defense, without any showing of relevance, which CIPA prohibits. *See* CIPA Section 4 Order at 11-12 (finding that "granting [the defendant] unfettered access to the Schulte Workstation and DEVLAN would gut the entire rationale of CIPA" and that the defendant was not "entitled to unfettered access" to these CIA computer systems). Furthermore, the Government did produce log files to the defendant from other CIA employees' workstations—on June 14, 2019, the Government produced log files from the workstations of employees who had Atlassian administrator privileges (*i.e.*, those individuals with the access required to access the Altabackups from which the Vault 7 Information was stolen). The defendant has never articulated why any other log files would be material to the defense in any way, nor explained why he is entitled to all "vi-client logs." If the defendant thought that log files from other specific employees' workstations were material to his defense—such as Michael's—he should have raised it before the second week of trial.

3. [redacted] The defense claims that the defendant was prejudiced by not receiving the permissions for David's home folder on the NetApp Server, in which David had stored a copy of a Stash backup file. *See* Mistrial Motion at 10. The defendant, however, has known that David stored that backup file in his home folder since December 10, 2018, when the Government produced the 302s of David's interviews. Had the defendant thought this information was material to his defense, he should have followed the Court's suggestion in the CIPA Section 4 Order and requested the permissions specifically from the Government, rather than wait until well after David testified to raise this issue. In any event, the backup file stored in David's home folder is *not* the March 3, 2016 backup file that was disclosed by

WikiLeaks; rather, it is dated over a month and a half after the date of the data posted online.

4. The defense argues that they could not challenge Mr. Leedom's testimony about permissions on the NetApp Server. *See* Mistrial Motion at 10. As an initial matter, the Government provided the defendant with the NetApp Access Control Lists ("ACLs") showing permissions to folders that existed on the NetApp, including the Altabackups, and the defendant actually noticed a portion of the NetApp ACLs in his CIPA Section 5 Notice. In any event, the defense grossly overstates the extent of Mr. Leedom's testimony. Mr. Leedom did not purport to describe the permissions that were put in place on the NetApp Server in 2016. Rather, Mr. Leedom testified only that the defendant had tried to create a data store from the NetApp, received a "permission-denied error" from the server, and was thus unable to create the data store. (*See* Tr. at 986-87). He then further testified that such activity could be consistent with "white-listing" access control (*see id.* at 987), which was a concept raised in a 302 for David (*see* CLASSIFIED JAS_010454 (describing how "NFS access is controlled by IP address"), produced to the defendant on December 10, 2018. Moreover, as the defense noted, several 302s did suggest that there were lax permissions on the Net App Server, which is a point that the defense has and can explore on cross-examination of those witnesses (such as, for example, when defense counsel elicited from David that he had told the FBI that the Altabackups were "wide open," (*see* Tr. at 887)), Mr. Leedom, or through the defense expert's testimony.

5. The defendant argues that his counsel's cross-examination of Mr. Berger was inhibited because he did not have access to the March 3, 2016 Confluence backup files. As noted above, however, the Government produced that file to the defense in discovery.

6. The defendant complains that Mr. Leedom testified about unallocated space on the ESXi Server and argues that because the Government did not produce the mirror image of the ESXi Server, the defense had "no access whatsoever to this unallocated space." *See* Mistrial Motion at 11. Again, the defendant is simply wrong. The Government produced all of the portions of unallocated space for the ESXi Server about which Mr. Leedom testified to the defense in discovery on December 10, 2018 and June 14, 2019.

7. The defendant argues that without the mirror image of the NetApp Server, he could not demonstrate that the Altabackups could also have been accessed through a "CIFS" share. *See* Mistrial Motion at 11. Initially, the Government notes that in advance of trial, the Government offered to assist the defendant's expert in making videos like the ones made by the Government's expert showing, among other things, how to navigate to the backups. Had the defendant wanted to show access through a CIFS share, the defendant could have accepted that offer. The defendant

chose not to. Moreover, the defendant simply ignores that, as defense counsel elicited in cross-examination, David deleted the "CIFS" share on March 1, 2017, before WikiLeaks began to disclose the Vault 7 Information (and thus before the CIA had any reason to keep it). (*See* Tr. at 880-90). Thus, even had the defense been able to view the mirror image of the NetApp Server when the FBI initially seized it—after the initial leak—the "CIFS" file sought by the defendant would not have been on that image.

8. The defendant argues that he could not test the vulnerability of the "DS00 file system," without access to the mirror image of the NetApp Server. The defendant does not explain why this forensic artifact would demonstrate any vulnerabilities or how any part of Mr. Leedom's testimony—which did not reference the file system—implicated this assertion. Therefore, the defendant has not established that a mistrial is required based on this claim.

9. The defendant argues that had he had access to the Net App Server, then he would not have alerted the Government to the devastating fact that the March 3, 2016 backup file was last accessed during the defendant's April 20, 2016 reversion of the Confluence virtual machine. The defendant cites to no authority that supports any relief, much less a mistrial, on this basis. The Government provided that information in response to a defense request well before trial, and the defendant cannot now seek to use that to derail a pending trial.

10. Finally, the defense complains that he should have been able to examine the Confluence virtual machine to determine whether another user had "root" access, such as Michael. Again, the defendant's argument fails. Initially, the defendant has been on notice since December 10, 2018 that Michael had "root" access to the ESXi Server, given that that fact was referenced in three different 302s produced to the defense at that time. Moreover, the defense has been provided with the available ESXi Server logs in discovery, such that he could have tried to determine whether any other user was logged in using the "root" password (there was not any such other user logged in during the reversion). Furthermore, to extent the defendant is complaining about the Confluence log files specifically, his assertion fails for two reasons. First, the Confluence log files of the activity on the Confluence virtual machine were deleted *when the defendant reversed the reversion*. Second, the Government produced to the defense the remaining Confluence application logs from April 7, 2016 through April 25, 2016 on June 14, 2019.

The case law cited by the defense simply does not support his request for the "drastic" remedy of a mistrial. For example, the defendant cites to *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016). *Ganias*, however, involved the question of whether law enforcement agents properly retained mirror images of hard drives seized pursuant, to a search warrant and its discussion of the various attributes of forensic evidence was dicta. *See* 824 F.3d at 210-216.

Moreover, in that case, the specific language upon which the defendant relies discusses the potential need for the defense expert to review forensic images to challenge the authentication of the evidence, *see id.* at 215—here, however, far from challenging the authenticity of the CIA forensic material, the defendant stipulated to it (*see* GX 3005). Similarly, in *United States v. Kimoto*, 588 F.3d 464 (7th Cir. 2009), the court found that there was no *Brady* violation, because, even if the Government had withheld full forensic images, the defendant was not prejudiced because the defendant did not take advantage of the material that the Government did provide. *See* 588 F.3d at 488 ("Thus, again, any prejudice to Mr. Kimoto resulted from his own failure to review the digital information in a timely fashion and to seek the court's assistance when he realized that there had been a misunderstanding with respect to the extent of the digital evidence in his possession."). So too here. While the defendant has maintained his stubborn insistence on full forensic images, he has failed to actually make use of the information the Government provided, such as the data on the Standalone, to explain why the discovery produced by the Government was inadequate, or to take the Court up on its repeated invitation to the defense to make more narrow requests. In *United States v. Hill*, the court did order the Government to produce two mirror images of hard drives containing child pornography to the defense. *See* 322 F. Supp. 2d 1081, 1091 (C.D. Cal. 2004). *Hill*, however, does not involve the requested disclosure of an unprecedented and staggering amount of classified information without a showing that the information would be both "relevant and helpful," as required by CIPA.[2] *See Aref*, 533 F.3d at 80. *United States v. Shrake*, which also involved the production of forensic material in a child pornography case and not one involving classified information, addressed a situation where the Government had retained a private expert and provided that expert with a mirror image of a computer hard disk outside of government facilities, in violation of the restrictions on such material imposed by the Adam Walsh Child Protection and Safety Act, while denying the defense expert the same production. *See* 515 F.3d 743, 746 (7th Cir. 2008). Again, that is not the case here—even setting aside the manifest difference in child pornography and espionage prosecutions, the Government did not violate any laws to give its experts preferential access to the data.[3]

---

[2] [redacted] *Hill* was also decided before the Adam Walsh Child Protection and Safety Act was passed in 2006, which added 18 U.S.C. § 3509(m), a provision of the Federal Criminal Code that now specifically prohibits the relief granted in *Hill*.

[3] [redacted] The defendant also cites two civil cases in support of his argument, but neither are helpful. *Santiago v. Miles* involved the production of a printout of data from a bank computer system, not the forensic image of the computer system itself. *See* 121 F.R.D. 636, 640 (W.D.N.Y. 1988) ("If the computer program was modified to generate a discrete set of documents for Cerio (see below), it may clearly be modified to generate a printout containing the raw data plaintiffs need . . . .). And in *Gates Rubber Company v. Bando Chemical Industries, Ltd.*, the court was determining whether to impose sanctions for spoliation based on a party's failure to make a forensic image of a hard drive, not what forensic materials should be provided in discovery to a criminal defendant. *See* 167 F.R.D. 90, 112 (D. Colo. 1996).

CONCLUSION

For the reasons set forth above, the Mistrial Motion should be denied.

GEOFFREY S. BERMAN
United States Attorney

By: /s/
David W. Denton Jr. / Sidhardha Kamaraju /
Matthew Laroche
Assistant United States Attorneys
(212) 637-2744 / 6523 / 2420

Cc: Defense Counsel (by hand)