UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **CONCORD MANAGEMENT AND CONSULTING LLC,** **Defendant.**	**Crim. No. 18-CR-32-2 (DLF)**

GOVERNMENT'S MOTION TO SUBSTITUTE FILING

The United States of America respectfully requests that the Court substitute on its docket the document attached to this motion as Exhibit A for the government's opposition to defendant's motion for approval to disclose discovery pursuant to the protective order filed on January 30, 2019 (Dkt. No. 94). In support of this motion, the government states as follows.

On January 30, 2019, the government filed its opposition to defendant Concord Management and Consulting LLC's motion for approval to disclose discovery pursuant to the protective order. Dkt. No. 94. Shortly after the government filed, defense counsel drew the government's attention to the following sentence, which appears on page nine of the filing: "On October 22, 2018, the newly created Twitter account @HackingRedstone published the following tweet: 'We've got access to the Special Counsel Mueller's probe database as we hacked Russian server with info from the Russian troll case Concord LLC v. Mueller. You can view all the files Mueller had about the IRA and Russian collusion. Enjoy the reading!'" Defense counsel pointed out that this sentence could be read to suggest that the Twitter account broadcast a publicly-available "tweet" on October 22. In fact, the Twitter account @HackingRedstone began sending multiple private direct messages to members of the media promoting a link to the online file-sharing webpage using Twitter on October 22. The content of those direct messages was consistent

with, but more expansive than, the quoted tweet to the general public, which was issued on October 30. By separate filing, the government will move to file under seal the text of the direct messages. The online file sharing webpage was publicly accessible at least starting on October 22.

In the interest of precision and to ensure there is no ambiguity, the government respectfully requests that the Court permit the government to substitute the document attached as Exhibit A to this motion for the January 30 filing, currently docketed as Document Number 94. The document attached as Exhibit A amends the sentence quoted above and makes a corresponding edit to the first full sentence on page 11 and is in all other respects identical to the January 30 filing.

Respectfully submitted,

ROBERT S. MUELLER III
Special Counsel

By: /s/
Jeannie S. Rhee
L. Rush Atkinson
U.S. Department of Justice
Special Counsel's Office
950 Pennsylvania Avenue NW
Washington, D.C. 20530
Telephone: (202) 616-0800

JESSIE K. LIU
United States Attorney

By: /s/
Deborah Curtis
Jonathan Kravis
Kathryn Rakoczy
Assistant United States Attorneys
555 Fourth Street N.W.
Washington, D.C. 20530

JOHN C. DEMERS
Assistant Attorney General for National Security

By: /s/
Heather N. Alpino
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave. NW
Washington, D.C. 20530
Telephone: (202) 514-2000

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **CONCORD MANAGEMENT AND CONSULTING LLC,** **Defendant.**	**Crim. No. 18-CR-32-2 (DLF)**

GOVERNMENT'S AMENDED OPPOSITION TO DEFENDANT'S MOTION FOR APPROVAL TO DISCLOSE DISCOVERY PURSUANT TO PROTECTIVE ORDER

The United States of America respectfully opposes the motion of defendant Concord Management and Consulting LLC for approval "to disclose documents identified by the Special Counsel as 'sensitive' to Concord's officers and employees for purpose of preparing for trial." Dkt. No. 77, at 1.

This Court has previously found that "[t]he government has demonstrated good cause for restricting sensitive discovery." Dkt. No. 42, at 3. The defendant's present motion seeks leave to send that sensitive discovery to the Russian Federation, where it would be possessed by at least one indicted co-conspirator, Yevgeniy Prigozhin, who has not appeared before the Court, as well as other unnamed individuals who are outside the jurisdiction of this Court. For the reasons set forth below, and based on the information set forth in the government's *ex parte* submission, Concord's request to send the sensitive discovery to the Russian Federation unreasonably risks the national security interests of the United States.

Nothing has occurred during the pendency of this litigation to ameliorate these risks. On the contrary, the government's concerns are only heightened by the apparent release and manipulation of information produced to Concord as "non-sensitive" discovery in this case. As

discussed in more detail below, in October 2018, one or more actors made statements claiming to have a stolen copy of discovery produced by the government in this case. The subsequent investigation has revealed that certain non-sensitive discovery materials in the defense's possession appear to have been altered and disseminated as part of a disinformation campaign aimed (apparently) at discrediting ongoing investigations into Russian interference in the U.S. political system. These facts establish a use of the non-sensitive discovery in this case in a manner inconsistent with the terms of the protective order and demonstrate the risks of permitting sensitive discovery to reside outside the confines of the United States.

Nor has Concord articulated any change in circumstances in this prosecution that could balance against these risks. The government's position is not, as Concord states, that defense counsel should be "prohibit[ed] . . . from sharing" sensitive discovery "with Defendant Concord for purposes of preparing for trial." Dkt. No. 77, at 1. On the contrary, the government has already provided Concord—the only defendant to have appeared before the Court—with sensitive discovery, and the government has never sought to bar Court-approved individual officers and employees of Concord from reviewing sensitive discovery materials in the United States offices of Reed Smith under the security protections established by the Court's protective order. Indeed, the government does not oppose such a review even by indicted officers and employees of Concord, as their appearance in the United States would allow them to stand trial. The government has established good cause for the Court to impose these reasonable limitations on the means by which the officers and employees of Concord may review the sensitive discovery, including continued restrictions requiring that sensitive discovery be viewed in the United States.

PROCEDURAL BACKGROUND

On June 29, 2018, this Court entered a protective order that included provisions restricting

the disclosure of material designated by the government as sensitive. Dkt. No. 42. The protective order barred any individual or entity—including Concord officer Yevgeniy Prigozhin—other than the U.S. defense team from accessing, sharing, or discussing sensitive discovery materials absent the Court's approval. Dkt. No. 42-1, ¶ 11. The order further required that sensitive discovery materials be stored offline at the U.S. offices of Reed Smith LLP ("Reed Smith") and not be disclosed, transported, or transmitted outside the United States. *Id.* ¶¶ 14, 15, 18. The order also required that any person reviewing sensitive materials must be accompanied at all times by a designated and identified employee of a U.S. office of Reed Smith. *Id.* ¶ 15.

The Court explained that these restrictions were warranted based on its finding that "[t]he government has demonstrated good cause for restricting sensitive discovery." Dkt. No. 42, at 3. The Court noted that the sensitive discovery "includes information describing the government's investigative techniques, identities of cooperating individuals and companies, and personal identifying information related to U.S. persons who were victims of identity theft." *Id.* "These substantial considerations," the Court concluded, "constitute ample good cause for the imposition of a protective order." *Id.*

Finally, the Court included in the protective order a provision that would allow defense counsel to "seek ex parte approval to disclose sensitive discovery materials to others, including . . . Concord's individual officers and employees (including Prigozhin)." *Id.* at 4. The protective order clarified that the government's position with respect to such requests would be litigated by a firewall counsel who is not a member of the prosecution team. *Id.* "This process for evaluating individualized discovery requests," the Court stated, "will enable the Court to carefully balance the government's weighty national security, law enforcement, and privacy concerns against Concord's right to discovery under Rule 16." *Id.* at 5.

On December 20, 2018, Concord filed a motion for approval to disclose discovery designated by the government as sensitive to "Concord's officers and employees for purpose of preparing for trial." Dkt. No. 77, at 1. Neither Concord's motion nor its proposed order identifies any specific individual (other than Prigozhin) to whom defense counsel intends to disclose the sensitive discovery. In addition, neither the motion nor the proposed order identifies any particular piece of sensitive discovery that defense counsel wishes to disclose. Instead, Concord requests blanket authority to disclose any and all sensitive discovery to any officer or employee of Concord, including but not limited to Prigozhin. Moreover, Concord's motion appears to contemplate that the sensitive discovery will be available for these individuals to view in the Russian Federation, outside the jurisdiction of this Court to enforce the terms of the protective order. (The government has filed under seal a supplement to this opposition discussing the protocol proposed by Concord for this review filed under seal as an attachment to its motion.)

ARGUMENT

Federal Rule of Criminal Procedure 16(d)(1) states that "[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief" in regulating discovery. The good-cause standard set forth in Rule 16(d)(1) permits restrictions on the use of discovery by a defendant based on "the protection of information vital to national security." *United States v. Cordova*, 806 F.3d 1085, 1090 (D.C. Cir. 2015) (quoting Fed. R. Crim. P. 16(d) Advisory Committee's Note to 1966 Amendment to Former Subdivision (e)). Once a showing of good cause has been made by the party seeking the order, "the court has relatively unconstrained discretion to fashion an appropriate protective order." *United States v. Johnson*, 314 F. Supp. 3d 248, 251 (D.D.C. 2018). Under this rule, "a trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted

disclosure of the materials which they may be entitled to inspect." *Cordova*, 806 F.3d at 1090 (quoting *Alderman v. United States*, 394 U.S. 165, 185 (1969) (internal quotation marks omitted)).

Requests to limit discovery under Rule 16(d)(1) are subject to a "balancing of interests," *United States v. Williams Cos., Inc.*, 562 F.3d 387, 395 (D.C. Cir. 2009), with the government's showing of good cause weighed against any imposition that the proposed limitation would place on the defendant's Sixth Amendment right to present an effective defense. *United States v. Celis*, 608 F.3d 818, 829 (D.C. Cir. 2010).

In this case, the balancing of those interests requires that the defendant's motion be denied. As this Court has already recognized, the government's showing of national security, law enforcement, and privacy concerns establishes "ample good cause" for a limitation on the dissemination of sensitive discovery under Rule 16(d)(1). Dkt. No. 42, at 3. The government's *ex parte* filing in connection with this motion only further reinforces that showing. Moreover, events related to the handling of non-sensitive discovery that have taken place since the Court's entry of the initial protective order add more weight to the government's showing of good cause and further reinforce the need for tight control over sensitive discovery.

In its motion to amend, Concord has not made any particularized showing that would warrant revisiting the balance struck by this Court in the protective order. Nor does Concord explain why this Court should permit the sensitive discovery to be viewed and possessed outside the United States, beyond the jurisdiction of this Court to enforce the terms of the protective order. *See Alderman*, 394 U.S. at 185 (noting that the Federal Rules of Criminal Procedure allow a trial court to "place a defendant and his counsel under *enforceable orders* against unwarranted disclosure of the materials which they may be entitled to inspect," and stating that "[w]e would not expect the district courts to permit the parties or counsel to take these orders lightly" (emphasis

added)).

I. Good Cause Exists To Restrict Dissemination of the Sensitive Discovery.

A. The Sensitive Discovery Implicates Significant National Security and Law Enforcement Interests.

As this Court has already found, the national security, privacy, and law enforcement interests implicated by the sensitive discovery in this case "constitute ample good cause for the imposition of a protective order." Dkt. No. 42, at 3; *see United States v. Hausa*, 232 F. Supp. 3d 257, 261 (E.D.N.Y. 2017) ("Concern for national security undoubtedly qualifies as good cause" for purposes of Rule 16(d)(1).)

That finding was based on several considerations. First, the sensitive discovery identifies uncharged individuals and entities that the government believes are continuing to engage in operations that interfere with lawful U.S. government functions like those activities charged in the indictment. *See United States v. Fiel*, No. 10-CR-170-7-HEH, 2010 WL 3396803, at *1 (E.D. Va. Aug. 25, 2010) (granting motion for protective order permitting defendant to access certain "confidential or law enforcement sensitive" discovery related to ongoing investigation only at the courthouse in the presence of counsel). Second, information within the sensitive discovery identifies sources, methods, and techniques used to identify the foreign actors behind these interference operations. *See United States v. El-Mezain*, 664 F.3d 467, 522 (5th Cir. 2011) ("As the court recognized in [*United States v.*] *Yunis*, the Government may have an interest in protecting the source and means of surveillance that goes beyond protection of the actual contents of an intercepted conversation."); *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Hausa*, 232 F. Supp. 3d at 262

("It is widely accepted that the Government has a compelling interest in protecting not only the content of classified materials, but also the sources, methods, and liaison relationships used to obtain them.") Unwarranted disclosure of that information overseas, in a country adverse to this litigation, would allow that country and actors in that country to learn of these techniques and adjust their conduct, thus undermining U.S. national security interests, including investigations into the conduct of those foreign actors.

The Court's protective order addressed these concerns by requiring that the sensitive discovery be stored offline in defense counsel's offices and by restricting the review of sensitive discovery to the U.S. defense team in the first instance. Dkt. No. 42-1, ¶¶ 14, 15, 18. However, the protective order did not absolutely preclude review of sensitive discovery by officers and employees of Concord. Rather, the protective order provided that defense counsel could request permission to show sensitive discovery to those officers and employees on a case-by-case basis, using firewall counsel if necessary to prevent the disclosure of defense strategy to the trial team. *Id.* ¶ 13.

Concord's motion does not make such a particularized request. Instead, Concord proposes to make the entirety of the sensitive discovery available electronically in Russia. Concord's proposed order would grant this access to "the officers and employees of Concord Management and Consulting LLC" without specifying who (or how many) those individuals are. The Court would have no ability to enforce compliance with the other provisions in the protective order by the "officers and employees of Concord Management and Consulting LLC" because those individuals are not subject to the jurisdiction of the Court. And Concord's proposed order would apply to every piece of sensitive discovery in the case, including sensitive discovery containing personal identifying information and sensitive discovery implicating national security interests. In

short, Concord requests that materials that this Court has already held implicate "important national security, law enforcement, and privacy interests," Dkt. No. 42, at 4, be disclosed to unnamed individuals in Russia who would have the ability to view and disseminate those materials and who would not be answerable to this Court for any violation of the protective order.

Concord argues that the government has "no further need" to protect ongoing investigative activity by restricting access to the sensitive discovery because a criminal complaint arising out of activity related to the conduct at issue in this case was recently unsealed in the Eastern District of Virginia. Dkt. No. 77, at 12-13. That argument is without merit. As set forth in the government's *ex parte* submission, the complaint filed in the Eastern District of Virginia does not obviate the interests implicated by the proposed release of the sensitive discovery.

In addition, Concord argues that restrictions on the sensitive discovery to protect investigative techniques are unnecessary because "any person anywhere in the world connected to the Internet already knows that law enforcement agencies can and do gather evidence from these types of companies through legal process in criminal matters, and specifically what can be gathered through those various processes is widely known and is not in need of protection." Dkt. No. 77, at 13-14. In support of that position, Concord cites to information available on the websites of particular service providers. This argument too is without merit, as the government also uses—and has used in this case—investigative techniques that are not widely known to the public, as explained in more detail in the government's *ex parte* submission.

B. The Mishandling of Non-Sensitive Discovery Highlights the Risks of Lifting Protections on the Sensitive Discovery.

The relief requested by Concord's motion—the authority to disclose sensitive discovery to unnamed employees and officers in Russia—is particularly unwarranted in light of recent events suggesting that non-sensitive discovery materials have been misused in a manner inconsistent with

the terms of the protective order.

On October 22, 2018, the newly created Twitter account @HackingRedstone began sending direct messages to Twitter accounts for members of the media claiming that the sender had access to "the Special Counsel Mueller database."[1] On October 30, 2018, the @HackingRedstone account issued a public tweet stating: "We've got access to the Special Counsel Mueller's probe database as we hacked Russian server with info from the Russian troll case Concord LLC v. Mueller. You can view all the files Mueller had about the IRA and Russian collusion. Enjoy the reading!" The tweet also included a link to a webpage located on an online file-sharing portal. This webpage contained file folders with names and folder structures that are unique to the names and structures of materials (including tracking numbers assigned by the Special Counsel's Office) produced by the government in discovery.[2] The FBI's initial review of

[1] On that same date, a reporter contacted the Special Counsel's Office to advise that the reporter had received a direct message on Twitter from an individual who stated that they had received discovery material by hacking into a Russian legal company that had obtained discovery material from Reed Smith. The individual further stated that he or she was able to view and download the files from the Russian legal company's database through a remote server.

[2] For example, the file-sharing website contains a folder labeled "001-W773." Within that folder was a folder labeled "Yahoo." Within that folder was a folder labeled "return." Within the "return" folder were several folders with the names of email addresses. In discovery in this case, the government produced a zip file named "Yahoo 773." Within that zip file were search warrant returns for Yahoo email accounts. The names of the email accounts contained in that zip file were identical to the names of the email address folders within the "return" subfolder on the webpage. The webpage contained numerous other examples of similarities between the structure of the discovery and the names and structures of the file folders on the webpage. The file names and structure of the material produced by the government in discovery are not a matter of public record.

At the same time, some folders contained within the Redstone Hacking release have naming conventions that do not appear in the government's discovery production but appear to have been applied in the course of uploading the government's production. For example, the "001-W773" folder appears within a folder labeled "REL001," which is not a folder found within the government's production. The naming convention of folder "REL001" suggests that the contents of the folder came from a production managed on Relativity, a software platform for managing

the over 300,000 files from the website has found that the unique "hashtag" values of over 1,000 files on the website matched the hashtag values of files produced in discovery.[3] Furthermore, the FBI's ongoing review has found no evidence that U.S. government servers, including servers used by the Special Counsel's Office, fell victim to any computer intrusion involving the discovery files.

The fact that the file folder names and folder structure on the webpage significantly match the non-public names and file structure of the materials produced in discovery, and the fact that over 1,000 files on the webpage match those produced in discovery, establish that the person(s) who created the webpage had access to at least some of the non-sensitive discovery produced by the government in this case.[4] Furthermore, the fact that some of the file structure on the webpage includes the "REL" file designation, which indicates the data was taken from a Relativity database, also suggests that the data was not taken from the Special Counsel's Office or the U.S. Attorney's Office, because the government has not used Relativity databases to store data related to this case. In addition, the dissemination of the link to the webpage via a Twitter message claiming to provide access to "all the files Mueller had about the IRA and Russian collusion" and the fact that the webpage contained numerous irrelevant files suggest that the person who created the webpage

---

document review. Neither the Special Counsel's Office nor the U.S. Attorney's Office used Relativity to produce discovery in this case.

[3] Most of the data within the unique folder names on the webpage was junk material that has nothing to do with this case. Also, the matching files found on the webpage do not appear to be located in the same file folders in which they were produced in discovery. In other words, the actual files are not located where they were otherwise located in discovery, but were instead mixed into the discovery, apparently randomly. The file-sharing portal webpage has since been deactivated after a request from the government.

[4] The 1,000+ matching files include images of political memes from Facebook and other social media accounts that, as alleged in the indictment, were posted and reposted online by the Internet Research Agency, and were produced in non-sensitive discovery. Many of those images are presumably still available elsewhere on the Internet.

used their knowledge of the non-sensitive discovery to make it appear as though the irrelevant files contained on the webpage were the sum total evidence of "IRA and Russian collusion" gathered by law enforcement in this matter in an apparent effort to discredit the investigation.

On October 23, 2018, defense counsel contacted the government to advise that defense counsel had received media inquiries from journalists claiming they had been offered "hacked discovery materials from our case." Defense counsel advised that the vendor hired by the defense reported no unauthorized access to the non-sensitive discovery. Defense counsel concluded, "I think it is a scam peddling the stuff that was hacked and dumped many years ago by Shaltai Boltai," referencing a purported hack of Concord's computer systems that occurred in approximately 2014. That hypothesis is not consistent with the fact that actual discovery materials from this case existed on the site, and that many of the file names and file structures on the webpage reflected file names and file structures from the discovery production in this case.[5]

As stated previously, these facts establish a use of the non-sensitive discovery in this case in a manner inconsistent with the terms of the protective order. The order states that discovery may be used by defense counsel "solely in connection with the defense of this criminal case, and for no other purpose, and in connection with no other proceeding, without further order of this Court," Dkt. No. 42-1, ¶ 1, and that "authorized persons shall not copy or reproduce the materials except in order to provide copies of the materials for use in connection with this case by defense counsel and authorized persons," *id.* ¶ 3. The use of the file names and file structure of the discovery to create a webpage intended to discredit the investigation in this case described above

[5] Defense counsel is aware of the internal reference numbers contained within the discovery productions (i.e., those leaked by the @HackingRedstone actor) and has referenced them in communications with the government to identify specific discovery productions.

shows that the discovery was reproduced for a purpose other than the defense of the case.

Moreover, consistent with the apparent pro-Russian aim of the tweet, to the extent that the individuals who created the webpage reside outside the United States,[6] this contravention is likely to go unpunished. Thus, this episode illustrates the danger of allowing sensitive discovery to be viewed and possessed by individuals who are beyond the jurisdiction of this Court. *Cf. Bittaker v. Woodford*, 331 F.3d 715, 726 (9th Cir. 2003) ("The power of courts . . . to delimit how parties may use information obtained through the court's power of compulsion is of long standing and well-accepted."). As the courts have recognized, these kinds of concerns about the possible misuse of discovery materials are best addressed by placing reasonable restrictions on where and how the defendant may view sensitive discovery materials. *See United States v. Fishenko*, No. 12-CR-626 (SJ), 6262014 WL 5587191, at *3 (E.D.N.Y. Nov. 3, 2014) (entering protective order allowing defendants to view sensitive national security materials only in the presence of counsel in isolation rooms at the jail); *United States v. Lindh*, 198 F. Supp. 2d 739, 743 (E.D. Va. 2002) (entering protective order prohibiting defense counsel from sharing certain sensitive unclassified information with detainees); *United States v. Moussaoui*, No. CRIM 01-455-A, 2002 WL 1311736 (E.D. Va. Jun. 11, 2002) (entering protective order prohibiting defense counsel from disclosing certain sensitive but unclassified material to the defendant); *United States v. Musa*, 833 F. Supp. 752 (E.D. Mo. 1993) (entering protective order allowing defendants to view sensitive national security materials only in the presence of counsel in isolation rooms at the jail); *see also United States v. Moore*, 322 Fed. Appx. 78, 83 (2d Cir. 2009) (affirming district court decision entering protective order allowing defendant to view certain discovery materials only in the presence of

[6] A representative of the online file-sharing portal has confirmed to the FBI that the specific account used to publish the matching discovery materials was registered on October 19, 2018 by a user with an IP address that resolves to Russia.

defense counsel); *United States v. Workman*, No. 18-CR-00020, 2019 WL 276843 (W.D. Va. Jan. 22, 2019) (upholding protective order issued by magistrate judge permitting defendant to access certain sensitive materials only in the presence of counsel); *United States v. Russell*, No. 15-CR-30005-DRH, 2015 WL 6460134, at *2 (S.D. Ill. Oct. 27, 2015) (restricting defendant's examination of discovery to offices of defense counsel based on government's showing of good cause); *Fiel*, 2010 WL 3396803, at *1 (granting motion for protective order permitting defendant to access certain "confidential or law enforcement sensitive" discovery only at the courthouse in the presence of counsel); *United States v. Guerrero*, No. 09-CR-339, 2010 WL 1506548, at *12-*13 (S.D.N.Y. Apr. 14, 2010) (granting motion for protective order providing that defendants may review certain discovery materials only in the presence of defense counsel and collecting cases granting similar motions).

Such restrictions are warranted based on a good-cause showing that discovery might be misused because, once sensitive discovery materials are provided to the defendant, "there is no telling where they will end up or what use (or misuse) might be made of them." *United States v. Mitchell*, No. 15-CR-00040-JAW-3, 2016 WL 7076991, at *3 (D. Me. Dec. 5, 2016) (granting government's motion for protective order requiring that certain discovery materials be viewed by the defendant only in the presence of defense counsel). Moreover, a protective order permitting defendants to view sensitive discovery materials only in the presence of defense counsel based on good cause shown is an appropriate restriction where, as here, "the underlying investigatory documents indicate that the defendants used several social media sites and related programs to communicate amongst themselves and with uncharged individuals," since "on-line social media affords a fast and efficient means of disseminating information to a wide group of recipients." *United States v. Johnson*, 191 F. Supp. 3d 363, 374 (M.D. Pa. 2016).

II. Concord Has Not Overcome the Government's Showing of Good Cause.

In the balancing of interests, Concord has not demonstrated that its ability to mount a defense at trial would be impaired by limitations on the dissemination of the sensitive discovery.

First, Concord argues that it "must be able to view and consider the discovery materials in order to evaluate and rebut any" evidence of Concord's intent "at trial." Dkt. No. 77, at 5. The problem with this argument is that Concord (through its counsel) has received the sensitive discovery materials and therefore can make use of them at trial. *See In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 126 (2d Cir. 2008) (concluding that "production of materials to a party's attorney alone falls within the common meaning of 'discovery'"); *United States v. Tounisi*, No. 13-CR-328, 2013 WL 5835770, at *2 (N.D. Ill. Oct. 30, 2013) (rejecting defendant's challenge to protective order permitting defense counsel but not defendant to view classified discovery on the ground that "counsel may prepare a defense with full access to the relevant and discoverable classified materials").[7] The issue before the Court is not whether or how Concord may use the sensitive discovery to defend itself, but rather the manner and the place in which Concord's officers and employees may view the sensitive discovery. Concord's motion

[7] While *In re Terrorist Bombings*, *Tounisi*, and several of the other cases cited in this opposition concerned discovery rulings in the context of the Classified Information Procedures Act ("CIPA"), the reasoning of those cases applies with equal force in this context, where the materials at issue are unclassified but sensitive for national security and law enforcement reasons. As the courts have recognized, CIPA is a "procedural statute" that was "intended to 'clarify' a court's existing 'powers under Federal Rule of Criminal Procedure 16(d)(1).'" *United States v. Mejia*, 448 F.3d 436, 455 (D.C. Cir. 2006) (citation omitted); *see also El-Mezain*, 664 F.3d at 520 (CIPA "clarifies the district court's existing power to restrict or deny discovery under the Federal Rules of Criminal Procedure."); *see also United States v. Rezaq*, 156 F.R.D. 514, 524 (D.D.C. 1994) (recognizing that both CIPA and Rule 16(d)(1) "authorize this court to issue protective orders" limiting disclosure of material to the defendant "to prevent disclosure of sensitive information that could compromise national security"), *vacated in part on reconsideration on other grounds*, 899 F. Supp. 697 (D.D.C. 1995). Therefore, it is appropriate to consider cases applying CIPA to similar discovery disputes in the context of this case, where the protective order entered by the Court was based on Rule 16(d)(1).

requests that every officer and employee of Concord be permitted to access every piece of sensitive discovery in Russia, where it is effectively impossible to secure the documents and where violations of the protective order are effectively beyond the jurisdiction of this Court to sanction. In light of the good cause showing made by the government, such unrestricted access is inappropriate, and Concord's generalized need to "evaluate and rebut" evidence is insufficient to overcome that showing.

Second, Concord argues that because the indictment alleges that Prigozhin is affiliated with Concord he must be permitted to view the sensitive discovery in order to "make informed decisions regarding its defense." Dkt. No. 77, at 5. But as this Court has already noted, "it is not clear that Prigozhin is the only individual with decisionmaking authority at Concord." Dkt. No. 42, at 2. Concord has not proffered any information about its structure that would shed light on this issue. Nor does Concord explain what sorts of decisions need to be made that require every officer and employee of Concord to have access to every piece of sensitive discovery in the Russian Federation.

Furthermore, Prigozhin is not precluded from accessing the sensitive discovery per se. He is subject to the same manner and place restrictions as all other Russian nationals. To the extent that Concord faces challenges in mounting its defense, it is because Prigozhin refuses to come to the United States to review the sensitive discovery. That is a problem of Concord's own making. After all, it was (apparently) Prigozhin's choice to have Concord enter an appearance in this criminal case, knowing that he was under indictment but declining to appear himself, let alone accept notice of the indictment. That circumstance—Concord defending itself in a criminal case in the United States with one of its officers refusing to travel to the United States to assist in the company's defense—may create a conflict between Prigozhin's interests and Concord's. One way

to resolve such a conflict is for the company to establish a litigation control group so that litigation decisions can be made on behalf of the company by those who do not have personal interests in the criminal case. Concord is under no obligation to organize itself in that way, but Concord also cannot complain about reasonable limitations on viewing sensitive discovery based on the personal interests of one of its officers. If Prigozhin chooses to remain outside the United States to avoid receiving notice of the indictment and to avoid responding to the charges as to him, then it is a reasonable limitation in light of the government's good cause showing to restrict the manner and place of Prigozhin's access to the sensitive discovery and to require Concord to "make informed decisions regarding its defense" in a manner that is consistent with those restrictions.

Third, Concord argues that its "officers and employees possess a critical first-hand understanding of its own business activities, and their input and insight about both is necessary for Concord to adequately prepare a defense." Dkt. No. 77, at 6. This argument is without merit. As discussed above, the courts have applied Rule 16(d)(1) to restrict the manner and means of dissemination of sensitive discovery to the defendant or to particular witnesses based on good cause shown. And in considering challenges to such restrictions, the courts have required a particularized showing from the defense as to how the disclosure of particular sensitive materials to the defendant or to a witness is necessary to the defense. *See In re Terrorist Bombings*, 552 F.3d at 118; *United States v. Al Fawwaz*, No. S7-98-CR-1023 (CAK), 2014 WL 6997604, at *3 (S.D.N.Y. Dec. 8, 2014) (denying challenge to protective order on the ground that defense "[c]ounsel have not identified particular" items of discovery "for which they have reason to believe" the defendant "could provide needed assistance"); *Hausa*, 232 F. Supp. 3d at 264 (rejecting challenge to protective order on the ground that "defendant has not articulated any non-speculative reason of how he would be able to help counsel understand the materials"); *Tounisi*,

2013 WL 5835770, at *2 (rejecting challenge to protective order prohibiting defendant from viewing classified discovery and noting that the defendant "fails to offer any tangible and material impairments to his ability to present a defense" and "fails to point to any specific evidence or instance where Tounisi's constitutional rights might be violated due to the procedure set forth in the" protective order). Concord's motion makes no such particularized showing, for example by identifying particular pieces of sensitive discovery that defense counsel proposes to show to particular employees or officers of Concord. (Under the terms of the protective order, any effort to make such a particularized showing should be filed under seal.)

Here again, at bottom, Concord's argument amounts to a complaint that its interests differ from those of its individual officers and employees, who would prefer for personal reasons not to come to the United States and subject themselves to the Court's jurisdiction in order to view the sensitive discovery. But the personal interests of Concord's officers and employees do not outweigh the government's showing of good cause for limitations on the manner in which the sensitive discovery is viewed and disseminated.

CONCLUSION

For the reasons stated above, the government respectfully requests that the Court deny Concord's motion regarding sensitive discovery.

Respectfully submitted,

ROBERT S. MUELLER III
Special Counsel

By: /s/
Jeannie S. Rhee
L. Rush Atkinson
U.S. Department of Justice
Special Counsel's Office
950 Pennsylvania Avenue NW

JESSIE K. LIU
United States Attorney

By: /s/
Deborah Curtis
Jonathan Kravis
Kathryn Rakoczy
Assistant United States Attorneys
555 Fourth Street N.W.

Washington, D.C. 20530
Telephone: (202) 616-0800

Washington, D.C. 20530

JOHN C. DEMERS
Assistant Attorney General for National Security

By: /s/
Heather N. Alpino
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave. NW
Washington, D.C. 20530
Telephone: (202) 514-2000

Attorneys for the United States of America