U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

February 15, 2011

VIA ECF

Honorable Richard D. Bennett
United States District Court
for the District of Maryland
101 West Lombard Street
Baltimore, Maryland 21201

Re: United States v. Thomas Andrews Drake
Case No. 10 CR 00181 RDB

Dear Judge Bennett:

This letter shall respond to the defendant's request for a two week extension to the February 25, 2011 deadline for serving expert disclosures and filing the defendant's notice of intent to disclose classified information under Section 5 of the Classified Information Procedures Act (CIPA).

This letter also responds to the defendant's request for formal discovery on a discrete matter. The government agrees that this request raises a disturbing issue, but, as described in detail below, not for the reason stated by defense counsel.

The government agrees that a status conference should be held. The Court, however, should deny both requests.

Introduction

As the government understands the request, the defendant bases his request for a two-week extension on three grounds. First, the defendant states that he needs "certain documents concerning the DOD IG investigation." *See* Dkt. 45, p. 2. Second, the defendant states that the defense classification expert has not completed his review of the classified evidence. *Id*. Third, the defendant states that the defense computer forensic expert's background investigation had not been completed until this week and, therefore, he or she has not accessed the classified discovery. *Id.*

Preliminarily, the government notes that the current filing date was a deadline selected by the defendant. *See* Dkt. 43. The government had recommended February 18th, but agreed to the defendant's request of February 25th. At the time the defendant selected this deadline, the

defendant must have known of the existence of all of these issues. For example, the defendant himself has known of his purported assistance with the Department of Defense Inspector General ("DOD IG") investigation and the fact that he provided documents to the DOD IG investigators for at least five years. Presumably, the defendant had shared these basic facts with his defense counsel.

As of December 21, 2010, the date of the last status conference, the defendant had not even contemplated the use of a classification expert. It was the defendant's need to obtain a classification expert that forced the original one month continuance. Finally, the defendant must have know that their computer forensic expert had not cleared his or her background investigation at the time the defendant requested the deadline. Therefore, none of these issues were unique or unforeseeable to the defendant at the time.

The DOD IG Investigation

The problem with the defendant's discovery request, which seeks documents allegedly provided to the DOD IG pursuant to its previous audit of a classified program, is several fold. First, many of the documents the defendant provided to the DOD IG were sent by attaching electronic copies of the documents to emails he sent to the DOD IG auditors, and the defendant is already in possession of these materials. The defendant has had electronic copies of emails and documents that he sent to the DOD IG since October 15, 2010. That was the day that the government installed a mirror image of the defendant's NSA computer account onto a viewing station in the defense SCIF. Although defense counsel had difficulty viewing portions of the viewing station until November 28, 2010, as the government recalls, these technical issues related to the defendant's home computer. As far as the government understands, the emails and attachments sent to the DOD IG were not affected, and these have been accessible to the defendant for the past four months, and most certainly for the past two and a half months. To date, the government understands that the number of DOD IG emails and document attachments located in the defendant's NSA computer account exceeds approximately a hundred and fifty (150) items.

Second, as to any hard copy documents provided by the defendant to the DOD IG, his request assumes that the DOD IG can trace back and segregate which documents in its possession were received from the defendant. Today, we learned that the DOD IG cannot segregate out hard copy documents provided by the defendant. In addition, most of the hard copy documents related to the audit were destroyed before the defendant was charged, pursuant to a standard document destruction policy. There was, for example, a notebook of documents provided by the defendant, many of which had nothing to do with the IG's audit, but this notebook was destroyed before the case began, and after the IG completed its audit. Moreover, it is entirely speculative that any hard copy documents provided by the defendant are different than or not merely cumulative of the electronic documents that the defendant already has.

Finally, there is no need to further extend the defendant's filing deadlines because the

government believes that the DOD IG documents are irrelevant and immaterial to this case, even under the discovery standard provided for by Rule 16 of the Federal Rules of Criminal Procedure and the government's expansive approach to providing discovery. This case is about the willful retention of classified documents at the defendant's residence. NSA required the defendant, like all of its employees, to follow a set of procedures and to seek approval from the appropriate individuals within NSA before bringing any documents home from NSA. An individual's assistance with an IG investigation is no exception to those clear rules. Therefore, what documents the defendant provided to the DOD IG have no bearing on the present charges. Of course, the resolution of this issue is exclusively within the Court's jurisdiction, and the government believes that it is quite likely that the Court will have to rule on this very issue in the near future.

Defense Classification Expert

As an initial matter, the defendants should have received all of the relevant, redacted classification guides by today's date. The additional discovery is not voluminous. The pages of the relevant, redacted classification guides are approximately fourteen pages. The government understands that the defense classification expert is scheduled to return to the defense SCIF this week. Therefore, the defense classification expert has ample time to finish his or her review and prepare a summary report.

The Section 5 filing requires notice of all classified documents that the defendant intends to use at trial. It is not limited to only those documents upon which the defense classification expert may rely. It is any document or information that the defendant reasonably expects to disclose at trial or any pretrial proceeding. Therefore, whether or not the defense classification expert has completed his or her summary, it is difficult to understand how, having extended the trial date once and with the current trial date only two months away from the February 25th filing date, the defendant does not already reasonably expect to use certain classified documents or information at this time.

Computer Forensic Expert

Other than an oral disclosure made by defense counsel on February 9th, this the first time that the government has learned that the background investigation of the defendant's computer forensic expert has not been completed. As the Court may recall, it ordered the initiation of this background investigation back on October 26, 2010. *See* Dkt. 29. The government had agreed to the initiation of the background investigation while the parties litigated the "need to know" issue back in November 2010 so that the background investigation could not be used as a basis for further delay.

The Court should make further inquiry regarding the reasons for the delay. If the delay is the fault of the expert, i.e. not returning paperwork or not responding to additional inquiries promptly, then this is no excuse for delay. Neither the Court nor the parties should be held

hostage to the expert's "other clients and matters he is juggling" or be "at the mercy of his schedule."

Finally, the defendant had requested background investigations for two computer forensic experts. *See* Dkt. 29. The defendant's February 12th filing only refers to a single "forensic computer expert." If the other computer forensic expert has completed his or her background investigation satisfactorily, then this is a further basis to deny the two week extension.

NSA Phone Calls to Mr. Drake

On December 23, 2010, counsel for the defendant reported to the government that their client had received two phone calls to his cellular telephone number from two number that his counsel believed belonged to NSA. The defendant received the telephone calls on December 15, 2010 at 2:50 p.m. and 2:57 p.m. Although not mentioned in their recent filing, the telephone calls were hang-ups. Counsel for the defendant represented that neither they nor their client knew who had called the defendant. The government referred the information to NSA's Office of General Counsel and immediately agreed to look into the matter. On December 24, 2010, the government received the defendant's cellular telephone number and the two telephone numbers that called his cellular telephone number from defense counsel.

Thereafter, the government expended many man-hours trying to ascertain whether the telephone numbers in fact belonged to NSA and to whom the numbers had been assigned. This included time expended by not only one of the principal investigators assigned to the underlying criminal case, but also security and telephone officials within NSA and the NSA affiliate. The government expended this time and effort based upon the repeated representations by defense counsel, both explicit and implicit, that their client did not know who had called him.

Curiously, in a conversation with defense counsel on January 24, 2011, defense counsel informed the government that counsel had reason to believe that the telephone numbers came back to the U.S. Cyber Command. When asked how counsel knew that fact, counsel declined to provide the basis for their information at that time. Thus, as of January 24th, defense counsel somehow was aware of a possible source for the telephone numbers before the government had even learned that fact.

By February 4, 2011 and through yesterday, the government had determined the following. The two telephone numbers had been subscribed, beginning in November 2010, to the Marine Corps Cyber Command[1] located in Columbia, Maryland. The Marine Corps Cyber Command ("MCCC"), a service component within the United States Cyber Command, has never

[1]The government did not identify the entity by name in its February 4th letter to defense counsel because it had to determine whether the entity's name was classified.

had any role or involvement in the investigation or prosecution of this matter.[2]

One of the two telephone numbers came back to the desk of a former employee of the MCCC. We determined that this employee was working there on December 15, 2010. This employee no longer works for the MCCC. The employee's last day of work was January 6, 2011. Colleagues of this former employee have told investigators that he also stated that he was testifying against the NSA in an unspecified, upcoming case. No member of the prosecution team, which includes the prosecutors and agents, ever gave this employee the defendant's number.[3]

The other telephone number had a wiring problem. When called, the number rang to the NSA operator even though the number has been subscribed to the MCCC. This number, however, did come back to an unassigned cubicle located within the MCCC and next to the office or cubicle of the former employee.

Based upon the defendant's February 12, 2011 filing, on February 14, 2011, one of the principal investigators interviewed the former employee and specifically asked about any calls that the former employee may have made to the defendant on December 15, 2010. The former employee admitted that he had called the defendant. The former employee further stated that he had known the defendant for many years and described the defendant as "a very good friend." The former employee then hung up on the investigator.

As further evidence of the close and historical relationship between the defendant and the former employee, we now have identified hundreds of emails (estimated as over five hundred (500)) on which both the defendant and the former employee appear. These emails span the time frame 2002 through 2007.

It is incomprehensible that the defendant would use his defense counsel to perpetrate a fraud upon this court. His defense counsel clearly had no idea that the defendant knew who this

---

[2]For purposes of framing the disputed legal issue, i.e. an unauthorized contact with a represented party, the government erred on the side of caution and identified the MCCC as a NSA affiliate in its February 4th letter to defense counsel. The government did so because NSA provides logistical and other support to the MCCC, and the Director of NSA has overall authority over the United States Cyber Command. The government understands, however, that the MCCC hires and fires its personnel, issues and revokes security clearances for its personnel, and performs many other functions independent of NSA.

[3]In light of the former employee's departure, we declined to provide the name of this individual to defense counsel due to Privacy Act concerns. *See* 5 U.S.C. § 552a(b). The government believes that the information obtained on February 14th and subsequent thereto only reinforces our judgment in this regard.

former employee was, but rather were quite properly representing the defendant's interests zealously. Nonetheless, the government wasted countless hours on this "fool's errand," and the parties were poised to expend even more of their time and potentially the Court's resources on this baseless allegation. Needless to say, there cannot be a violation of the "contact with a represented party" rule when the very contact at issue was from the defendant's "very good friend."

Given this most recent information, we expect defense counsel to withdraw their discovery request promptly.

Very truly yours,

/s/

William M. Welch II
Senior Litigation Counsel
John P. Pearson
Trial Attorney
Public Integrity Section
United States Department of Justice