**U.S. Department of Justice**

Office of the Inspector General

March 6, 2020

Colton Kells
Civil Liberties and Transparency Clinic
University at Buffalo School of Law
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
coltonke@buffalo.edu

Jonathan Manes, Esq.
Roderick & Solange MacArthur Justice Center
160 E. Grand Ave., Sixth Floor
Chicago, IL 60611
jonathan.manes@law.northwestern.edu

Re: Freedom of Information/Privacy Act Request [18-OIG-505]
*Privacy International, et al. v. FBI, et al.*, No. 18-cv-1488 (W.D.N.Y.)

Dear Messrs. Manes and Kells:

This responds to your request under the Freedom of Information Act (FOIA) for access to records maintained by the Department of Justice (DOJ) Office of the Inspector General (OIG). Specifically, you seek copies of "[a]ny reports…arising out of an investigation, internal inquiry, audit, evaluation or other oversight activity that concerns hacking techniques or the use of equipment, software and/or technology that implements or facilitates hacking techniques." The second part of your request seeks "[a]ny records that the OIG relied upon in the course of preparing reports or other documents responsive to" the first part of the request. This letter supplements our response made to you on September 28, 2018.

Through a search, as stated in the September 28, 2018 letter, OIG identified its publicly available report entitled "A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation," (OIG Report) as responsive to your request. As part of the above-referenced litigation, and as stated in the January 31, 2020 Joint Status Report, the parties agreed that with respect to the second part of your request, OIG would process any records that OIG relied upon in the OIG Report's discussion of FBI's use of a Computer and Internet Protocol Address Verifier ("CIPAV"), such as the discussion on portions of pages 11 through 16, as well as the five records identified in your November 5, 2019 letter in the litigation, or, the discrete portions thereof, as applicable, that are in OIG's files. Other than the documents noted herein and agreed upon by the parties, our search located no additional documents responsive to your request.

We have determined that certain portions of such documents should be withheld from disclosure pursuant to FOIA exemptions, 5 U.S.C. §552(b)(6), (b)(7)(C), and (b)(7)(E) as follows:

- 5 U.S.C. § 552(b)(6), protects personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- 5 U.S.C. § 552(b)(7)(C), protects records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information could reasonably be expected to constitute an unwarranted invasion of personal privacy; and
- 5 U.S.C. § 552(b)(7)(E), protects records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information would disclose techniques and procedures for law enforcement investigations or prosecutions, or would Road-disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Consequently, enclosed are records which can be released pursuant to your request. We have sent for consultation portions of four (4) pages of these records that contain information of substantial interest to the Federal Bureau of Investigation (FBI). We will inform you regarding our determination following this consultation.

We also located twenty-one (21) documents consisting of approximately 150 pages that originated with the FBI. We have referred these documents to the FBI for processing and direct response to you.

Finally, we located one document consisting of approximately twenty-two (22) pages that originated with the Office of the Attorney General. We have referred this document to DOJ Office of Information Policy for processing and direct response to you.

If you are not satisfied with OIG's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact our FOIA Public Liaison, Deborah Waller at (202) 616-0646 for

any further assistance of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at 1-877-684-6448.

Sincerely,

***Jacqueline E. Lightle***
Government Information Specialist
Office of the General Counsel

Enclosures

| Case Number: | Reporting Office: |
|---|---|
| E2014019 | OFFICE OF OVERSIGHT AND REVIEW |

Re: Telephonic interview of (b) (7)(C), (b) (6) Assistant Special Agent in Charge (ASAC), Federal Bureau of Investigation (FBI), Department of Justice (DOJ).

Investigative Counsel (b) (7)(C), (b) (6) telephonically interviewed (b) (6), (b) (7)(C) on March 10, 2015 at approximately 12:50PM EST, in connection with a review of the FBI's impersonation of the Associate Press in an undercover matter intended to identify an unknown subject. Also present was Program Analyst (b) (6), (b) (7)(C). IC (b) (6), (b) (7)(C) and (b) (7)(C), (b) (6) were located at 1425 New York Avenue, 13th Floor, Washington D.C., while (b) (7)(C), (b) (6) was located in Oregon.

(b) (6), (b) (7)(C) was sworn in.

IC (b) (7)(C), (b) (6) summarized that the OIG was looking to claims by the Associated Press regarding a case involving Timberline high school student (b) (7)(C), (b) (6), who utilized a false IP address to send a series of bomb threats to his high school. The Seattle police department requested the FBI Seattle Division's assistance in identifying (b) (7)(C), (b) (6), which they accomplished by surreptitiously inserting a tool known as a CIPAV onto (b) (7)(C), (b) (6) computer to track his IP address.

(b) (7)(C), (b) (6) **Professional Background**

(b) (7)(C), (b) (6)

**Seattle Division – Timberline Bomb Threat Investigation**

[00:03:45] (b) (6), (b) (7)(C) was asked if he recalled working with Special Agent (b) (7)(C), (b) (6) during his time as the ASAC of the Seattle Division. (b) (7)(C), (b) (6) responded yes, and explained that (b) (7)(C), (b) (6) was a Supervisory Special Agent in charge of a squad that investigated cybercrime.

| Special Agent Name and Signature: | (b) (7)(C), (b) (6), Program Analyst | Date: 03/10/2015 |
|---|---|---|

(b) (7)(C), (b) (6) was asked if it was common for (b) (7)(C), (b) (6) to brief him on the cases he was working. He responded yes, adding that this was especially true for cases that required authorizations or approvals above his level. When asked to elaborate, (b) (7)(C), (b) (6) explained that there were certain subpoena requests or electronic eavesdropping requests that required authorization before applications could be submitted to the court.

(b) (7)(C), (b) (6) was asked if he was ever delegated the responsibility for approving undercover operations. He responded that he could be delegated the authority by the SAC, but that the SAC was ultimately responsible. He added that he would review requests for undercover operations, but repeated that those were ultimately approved by the SAC.

[00:05:45] (b) (6), (b) (7)(C) was asked if he recalled being briefed by SSA (b) (6), (b) (7)(C) regarding bomb threats against Timberline High School. He stated that his recollection is extremely limited, adding that he had no independent recollection of the investigation other than a vague recollection of the name of the school. He added that he knew (b) (7)(C), (b) (6) would brief him on investigations such as the one that IC (b) (7)(C), (b) (6) described, but reiterated that he had no independent recollection of the Timberline bomb threat investigation.

IC (b) (7)(C), (b) (6) informed (b) (7)(C), (b) (6) that those were the only questions he had, and asked if (b) (7)(C), (b) (6) would be willing to speak with the OIG again if needed. (b) (7)(C), (b) (6) agreed, and provided additional contact information.

[00:07:25] (b) (6), (b) (7)(C) added that he wanted to state on the record that he is "absolutely positive" that whatever briefings he received from SSA (b) (6), (b) (7)(C) were for investigations that they believed were not only legal, but ethical and necessary to conduct. He added that he (b) (7)(C), (b) (6)

**Record Ends**

| Case Number: | Reporting Office: |
|---|---|
| E2014019 | OFFICE OF OVERSIGHT AND REVIEW |

Re: Voluntary interview of (b) (6), (b) (7)(C) [redacted] (b) (6), (b) (7)(C) Federal Bureau of Investigation (FBI), Department of Justice (DOJ).

Investigative Counsel (b) (7)(C), (b) (6) interviewed [redacted] on March 24, 2015 at approximately 2:00PM EST, in connection with a review of the FBI's impersonation of a member of the Associated Press in connection with an undercover matter intended to identify an unknown subject. Also present was Program Analyst (b) (7)(C), (b) (6) The interview took place in OIG offices at 1425 New York Avenue, 13th Floor, Washington D.C.

[redacted] was sworn in, and informed that he was not presently a subject in the OIG investigation.

**Professional Background**

(b) (7)(C), (b) (6) [redacted]

[redacted] **Work with the Seattle Division and Cyber Unit**

[00:04:00] [redacted] was asked to describe the reporting chain at the Seattle Field Division, and he explained that there was a Special Agent in Charge (SAC), an Assistance Special Agent in Charge (ASAC), and (b) (6), (b) (7)(C) [redacted] a field supervisor. He added that there were agents, analysts, and professional support, then supervisory special agents and supervisory intelligence analysts, and then ASACs and the SAC.

| Special Agent Name and Signature: | (b) (7)(C), (b) (6), Program Analyst | Date: 03/24/2015 |
|---|---|---|

When asked about the Cyber Unit (b) (6), (b) (7)(C), [redacted] explained that it was a Computer Investigations Unit that investigated hacking, child pornography, intellectual property rights violations and fraud. (b) (6), (b) (7)(C) the Digital Forensics Program, which was the recovery of all digital information from computers, recorders, or cameras. (b) (6), (b) (7)(C) [redacted]

[00:05:45] When asked if he was familiar with the Northwest Cyber Crimes Task Force (NWCCTF), [redacted] responded yes and added that it was in place when he started in Seattle. He explained that the task force consisted of the Washington State Patrol and the FBI, and the intent was to build the task force by bringing in other local law enforcement. He added that it was more of a (b) (7)(E) [redacted] the Washington State Patrol was the NWCCTF's most involved partner, and Detective (b) (6), (b) (7)(C) [redacted] could do both cyber investigations and forensics.

When asked if the FBI was in charge of the NWCCTF, or if it was jointly run by the two agencies, [redacted] explained that it was housed in FBI space, and FBI provided most of the training and resources. When asked if he was in charge of the NWCCTF when he was there, and the members essentially reported to him, [redacted] responded yes.

**Timberline High School Bomb Threats**

[00:07:45] [redacted] was asked if he recalled how the FBI became involved in the Timberline High School investigation. He explained that the Lacey Police Department contacted the FBI through Detective (b) (6), (b) (7)(C) because they knew him and his forensic capabilities. [redacted] added that Seattle division had had a number of school bomb threats and e-mails while he was there, but the Timberline investigation was the only one in which the unknown subject (UNSUB) deliberately attempted to use a proxy to obfuscate where they were. Therefore, Timberline was unique in that respect. [redacted] explained that typically they would have a kid post an online threat, (b) (7)(E) [redacted] With the Timberline threats, however, the UNSUB used a proxy in Italy to access a fake e-mail account to send the threats, which suggested a level of sophistication that was not typical.

[00:09:45] [redacted] was asked to briefly describe what he meant by "proxy." He explained that when you log into your e-mail, you go from your home computer to your e-mail application. A proxy, on the other hand, involves using your computer to access another computer or system (the proxy), and using that computer or system to access your e-mail application. When asked if the goal of using a proxy was to

essentially hide one's location or identity, [redacted] agreed that it can be. When asked if the UNSUB in the Timberline threats—who was later revealed to be a student named (b) (7)(C), (b) (6) —was using a proxy in Italy to hide his location, [redacted] responded yes and added that the proxy in Italy was used to send the threats.

[00:11:00] [redacted] was asked if, once he was contacted by Lacey PD, (b) (7)(C), (b) (6) came to him about the case. [redacted] responded yes, and stated that they went over the facts of what was happening at Timberline, including the methodology, threats, and the fact that the school had been evacuated. He added that the methodology of the threats suggested a level of technical knowledge that made the Cyber Unit the best equipped unit to help. In addition to the bomb threats, the UNSUB also launched a Denial of Service attack on Timberline High School web site. This involved the UNSUB using the proxy in Italy to bombard the Timberline High School web site with so many requests for service that it crashed the site. [redacted] stated that both Denial of Service attacks and accessing another person's computer without their knowledge are federal violations, and added that they had enough predication to open an investigation.

When asked who from the Seattle Division worked on the Timberline High School investigation, [redacted] named (b) (7)(C), (b) (6) Intelligence Analyst (b) (7)(C), (b) (6) and Information Technology Specialist (b) (7)(C), (b) (6) added that (b) (7)(C), (b) (6) served as the case agent with (b) (7)(C), (b) (6) and stated that (b) (6), (b) (7)(C) handled all the documentation to minimize issues with warrants. When asked if (b) (7)(C), (b) (6) was essentially the lead case agent, [redacted] responded yes.

[redacted] was asked what roles (b) (7)(C), (b) (6) and (b) (7)(C), (b) (6) played, and he explained that [redacted] was the intelligence analyst who helped craft the ruse news report, and [redacted] handled a lot of the technological aspects, such as reviewing the logs and data yielded through a Pen Register Trap and Trace (PRTT).

[00:14:15] [redacted] was asked how much involvement he would have from a supervisory role in the day to day operations of the investigation. [redacted] responded that it depended on the case, and added that in the Timberline investigation the first couple of days consisted of setting things up, but right before they deployed the CIPAV he was there directly.

**Timberline Investigation**

[redacted] was asked if the investigative team came up with a plan for identifying the UNSUB in the Timberline case. He explained that they met with the Lacey PD for a briefing on what they knew, adding that Lacey PD had come up with a list of possible people involved. [redacted] added that it was not public knowledge that the FBI was

involved in the investigation, so Lacey PD would take a more overt role in interviews and surveillance, while FBI would pursue the technical angle.

Returning to the meeting between Lacey PD and the FBI, [redacted] was asked if [redacted] was on the list of possible subjects the Lacey PD had put together. He responded yes, and provided a chart that the team had used to map out the activity of the investigation [Bates APN_000070], including [redacted] and where IP addresses were located. [redacted] added that the three names listed as possible subject came up early in the investigation, but due to circumstances they never got to the point of targeting each subject with a PRTT. [redacted] was asked if it was correct that a trap and trace had resulted from the meeting, just not for [redacted] and [redacted] agreed. He indicated to one of the names, [redacted], and stated that they ordered a trap and trace at [redacted] He stated that they found [redacted] nothing that could trace back to the Timberline threats. Therefore they eliminated [redacted] as a suspect.

[00:20:15] [redacted] was asked if, at this meeting with Lacey PD, they made the decision to use a tool known as a CIPAV. [redacted] stated that the team knew that a CIPAV was an option. He added that, based on the activity in Italy, they were confident that someone in Washington State was using the Italy box [**OIG Note**: I believe he's referring to the Italy computer] to access their e-mail and send the threats. [redacted] added that they sent a lead to Rome requesting them to follow up, [redacted]

[redacted] stated that, ideally, they were trying to get a computer to search and then trace back to the originating computer. It was summarized that the FBI had identified computers in Italy, the Czech Republic, [redacted] stated that FBI and Lacey PD were exhausting their other traditional investigative steps with trap and traces of potential subject's computers, as well as physical surveillance and interviews. However, those traditional investigative techniques were not getting them any closer to identifying the UNSUB.

[00:23:45] With regards to using a CIPAV, [redacted] stated that the FBI knew that the UNSUB was using a Myspace account. [redacted]

(b) (7)(E) Therefore, they knew that an undercover communication was possible, and that they had an avenue to try and use a CIPAV if they got to that point. After some research into the CIPAV technique, they decided to pursue that option.

**Approvals and Guidelines for Undercover Activity**

[00:25:00] was asked if there was an internal approval process within the FBI that had to be followed before one could use a CIPAV. stated that there was an approval process for the undercover technique in general. (b) (7)(C), (b) (6) (b) (7)(C), (b) (6) He explained that at the time they followed the Field Guide for Undercover and Sensitive Operations (FGUSO) which was based on the Attorney General Guidelines for conducting undercover operations (AGG-UCO). Therefore, as a supervisor, he researched the undercover scenarios they were looking to execute to see if a sensitive circumstance existed, SENT TO FBI FOR CONSULTATION explained that he used the FGUSO to determine whether the undercover scenario they were considering would qualify as a sensitive circumstance.

[00:27:45] was informed that the OIG knew that at some point during the investigation his team contacted one of the Behavioral Assessment Units (BAU) in the Critical Incident Response Group (CIRG). When asked who reached out to the BAU, explained that he believed he did. He added that Timberline was not the first school threat Seattle Division had handled, so they had used BAU before. So he contacted the BAU around June 8, 2007, and they sat down and discussed the circumstance and background surrounding the case. The BAU's recommendation was that the UNSUB was narcissistic, and that a media angle may be a way to play on his or her ego.

When asked what the BAU meant by "media angle," explained it was something related to the news. He added that the UNSUB had posted statements on The Olympian, and was actively and overtly ranting at others, so the BAU thought that taking a media approach or posing as some sort of media entity could feed into his. explained that his investigative team had spent some time discussing the possible scenario, and that they had believed that posing as a reporter may be problematic because a reporter's name could be easily verified, as opposed to a publisher or editor whose name would not be readily out there.

[00:30:15] [redacted] was asked if, once the investigative team decided on the undercover scenario of posing as an editor or publisher, he went back to review the FGUSO to determine if the operation qualified as a sensitive circumstance. He responded yes. It was pointed out that the AGG-UCO outlines a sensitive circumstance as one where exists a "significant risk that a third-party will enter into a professional or confidential relationship with a person participating in an undercover operation who is acting as an attorney, physician, clergyman, or member of the news media." [redacted] stated that he reviewed the FGUSO, and concluded that the operation was not a sensitive circumstance because the only intention of the communication was to get the UNSUB to click on the link to activate the CIPAV. There was never any intention to publish anything. Based on the behavioral analysis, a news story could play on the UNSUB's ego, and the team's goal was to build enough credibility and rapport that the UNSUB would not think the link was a virus and not click on it. They planned to engage in only enough contact to build that credibility so he would click on the link and activate the CIPAV

When asked if he considered whether the operation posed a "significant risk," [redacted] responded that at the time nothing registered in his head as a sensitive circumstance. He added that after the fact he was able to see why the Associated Press would have been upset with the procedure.

[redacted]'s attention was directed to chapter three of the FGUSO, which details privileged relationships. [redacted] was asked if he considered whether the operation would have established a privileged relationship, and he responded that he could not say for sure. He reiterated that knew he read the chapter detailing sensitive circumstances, but did not identify anything that would have been a sensitive circumstance.

**[00:57:00]** At the end of the interview, [redacted] stated that he understood that the issues surrounding potentially sensitive circumstances of undercover operations was a policy issue. He added that doing the research into those policies and making the judgment call was his responsibility, and he did not want anyone else on the investigative team to feel any type of responsibility for that. It was his research, and if anyone should have called a time out it would have been him. [redacted] was informed that, from his testimony, he clearly researched and considered the issue of whether or not a sensitive circumstance existed, and subsequently concluded that it was not because the team's goal was to just develop a rapport with the UNSUB so he would click on the link. The fact that the FBI was posing as a member of the media was a means to that end.

[00:58:30] [redacted] attention was directed back to chapter three of the FGUSO, which covered privileged relationships, there was a note after the section that stated a privileged relationship exists if there is a "significant risk that a third-party will enter into a professional or confidential relationship with a person participating in an

undercover operation who is acting as an attorney, physician, clergyman, or member of the news media." The note reads: "The sensitive circumstances are listed in order to identify any operational scenario in which privileged communications or defense trial strategy might be overheard." When asked if he was concerned that the team would get a privileged communication from the UNSUB, [redacted] responded no. He added that they were not purporting to be an attorney, and stated that he understood the media portion but they had no intention to contact anyone else besides the UNSUB, (b) (7)(E) [redacted]. He further added that the behavior analysis and the assessment of the UNSUB's personality, as well as his engagement, never raised any flags that there might be an issue. Furthermore, they never intended to engage a third-party outside of the UNSUB. They just wanted to get the UNSUB to click on a link.

[redacted]'s attention was directed to the next line of text, which read: "a relationship with a subject is established which the subject believes to be privileged." [redacted] was asked if, to his knowledge, an individual could enter into a privileged relationship with a reporter, akin to an attorney-client privilege. He responded yes, if the individual is a source, but stated that he was not aware of a "reporter-source" privilege. [redacted] was asked if he had any concerns that the UNSUB would enter into or believe they were entering into a privileged relationship with the FBI's undercover agent. [redacted] responded no.

**Obtaining Approval for Undercover Activity**

[00:36:45] [redacted] was asked to describe how the CIPAV was going to be deployed, and he explained that the scenario involved the team communicating with the UNSUB and providing him with some form of communication that contained the link that would activate the CIPAV. Once the CIPAV is activated, it provided the computer's IP address and other computer information, which the FBI could use to identify the internet service provider and get the customer's address.

[00:38:05] [redacted] SENT TO FBI FOR CONSULTATION [redacted]

SENT TO FBI FOR CONSULTATION [redacted]

[00:39:30] [redacted] was asked who he sought approval from at the Seattle Field Division. He named [redacted] ASAC [redacted] and stated that in a briefing he informed [redacted] of the circumstances surrounding the investigation and what the team was trying to accomplish. In particular, he would have discussed the fact that the team was trying to get the subject to click on a link, that they did not anticipate more than three substantive contacts, and that they were not trying to get a face-to-face meeting. SENT TO FBI FOR CONSULTATION [redacted] was asked if during that meeting they discussed the media scenario, or whether sensitive circumstances existed. He stated that he was pretty sure they did, but added that he could not recall the exact conversation. He explained that the media angle was not something the investigative team kept under wraps, and added that he would have given [redacted] his opinion on whether sensitive circumstances existed based on the research he conducted. Given that he discussed the media angle and the issue of sensitive circumstances with [redacted] was asked if he recalled whether [redacted] raised any concerns during the briefing. [redacted] responded no.

When asked if ASAC [redacted] approved the undercover activity, [redacted] confirmed that he had. When asked if he knew whether ASAC [redacted] or the SAC advised HQ of the undercover activity before it occurred, [redacted] responded not to his knowledge.

**Implementing Undercover Activity and Deployment of CIPAV**

[00:43:10] When asked to describe what occurred after the approval, [redacted] explained that the team crafted the ruse article and sent [redacted] to the UNSUB's Myspace account on June 12, 2007, [redacted]. When asked if [redacted] was present during this exchange, or when [redacted] established contact with the UNSUB via e-mail, [redacted] explained that towards the end of the second day he was there the whole time. He added that he wrote some of the language in the affidavit on June 12th.

With regards to the affidavit, [redacted] was asked if he followed any of the recent news reports on the case. He responded that he saw some of them. It was pointed out that one of the issues raised was that the affidavit did not mention that the team was going to pose as news reporters. When asked if he would have put the particulars of an operation in an affidavit, [redacted] stated that he thought it depended on the circumstances, and he unfortunately did not remember the discussion with the judge. When asked if there was a requirement that an affidavit in support of Title III

applications should describe details of an operation or how it will play out, [redacted] responded that he was not aware of any such requirement. When asked if the affidavit was reviewed by AUSA [redacted], [redacted] responded yes and added that the team worked very closely with her. When asked if anyone from FBI legal reviewed the affidavit, [redacted] stated that he believed an attorney from the Operational Technology Division reviewed it as well.

[00:46:45] When asked to describe the events of June 13, 2007, [redacted] explained that [redacted] reached out to the UNSUB via his Myspace account and, initially, the UNSUB responded "leave me alone." However, once [redacted] explained that he wanted to get the UNSUB's story and version of events, the UNSUB began to engage in conversation. [redacted] explained that they were drawing on the recommendations from the BAU to play on the UNSUB's ego and build rapport so that he would click on the link. [redacted] was read an excerpt from one of the e-mail chats that [redacted] had with the UNSUB [APN_000098], and was asked to lay out how it built rapport. [redacted] explained that they knew that the UNSUB had posted a few stories online and was obviously trying to draw attention, and that his Myspace page also had a lot of activity. Therefore the team was trying to both feed into that desire for attention, as well as assure the UNSUB that they were only trying to tell his side of the story, not learn his identity. [redacted] added that they were trying to build credibility and get the UNSUB to believe [redacted] was who he said, and thus make it more likely that the UNSUB would click the link and activate the CIPAV.

[00:50:20] When asked if the UNSUB agreed to help, [redacted] responded yes. [redacted]s attention was directed to the subsequent chat conversations, particularly the message that included a link to the ruse article. When asked if that was the link that contained the CIPAV, [redacted] stated that believed so. He indicated to the notes from that day and pointed out that it said the CIPAV was deployed at 3:30pm. [redacted] added that the UNSUB did click on the link, but [redacted]

adding pictures to the article, and when the UNSUB clicked on the link the CIPAV deployed correctly and they were able to identify the IP [redacted] addresses. They provided that information to Lacey PD, [redacted]

**After the Undercover Activity**

[00:53:34] It was summarized that (b) (7)(C), (b) (6) was arrested and later charged at the local level. When asked if he knew why AUSA (b) (6), (b) (7)(C) chose to not prosecute (b) (7)(C), (b) (6) federally, (b) (7)(C), (b) (6) responded that it was because he was a juvenile.

[00:53:55] (b) (6), (b) (7)(C) attention was directed to an e-mail from Lacey PD (b) (7)(C), (b) (6) to (b) (7)(C), (b) (6) labeled [APN_001427], which was essentially a thank you note expressing Lacey PD's appreciation for the FBI's assistance. (b) (7)(C), (b) (6) stated that he believed (b) (7)(C), (b) (6) sent letters to everyone involved.

(b) (7)(C), (b) (6) was asked if, after the operation was completed, he or a member of his team sent HQ an EC notifying them of the success. (b) (7)(C), (b) (6) explained that they sent an Urgent Report to advise HQ of the events. When asked what the difference was between an Urgent Report and a standard report, (b) (7)(C), (b) (6) explained that it was a way to get information to HQ quickly no matter the time of day. It was pointed out that the report was actually addressed to the Director of the FBI, and (b) (7)(C), (b) (6) was asked if he knew whether it actually went to the Director. He responded that he did not know.

[00:55:45] (b) (6), (b) (7)(C) was informed that, after the news media got involved in the story in 2014, the Cyber Division of FBI put together a Situational Action Background (SAB) dated October 29, 2014. When asked if he had any involvement in crafting the SAB, (b) (7)(C), (b) (6) responded no, adding that (b) (7)(C), (b) (6) informed him that he was providing documents to the Cyber Division.

**Record Ends**

| Case Number: | Reporting Office: |
|---|---|
| E2014019 | OFFICE OF OVERSIGHT AND REVIEW |

Re: Compelled interview of (b) (7)(C), (b) (6) Special Agent with the Seattle Cyber Division, Federal Bureau of Investigation (FBI), Department of Justice (DOJ).

Investigative Counsel (b) (7)(C), (b) (6) interviewed (b) (7)(C), (b) (6) via a video teleconference on April 07, 2015 at approximately 1:15PM EST, in connection with a review of the FBI's impersonation of a member of the Associated Press in connection with an undercover matter intended to identify an unknown subject. Also present were Program Analyst (b) (7)(C), (b) (6) and Special Agent (b) (7)(C), (b) (6) counsel, (b) (7)(C), (b) (6) IC (b) (7)(C), (b) (6), Analyst (b) (7)(C), (b) (6) were located at OIG offices at 1425 New York Avenue, 13th Floor, Washington D.C, while (b) (7)(C), (b) (6) was located at the Seattle U.S. Attorney's Office in Washington State.

(b) (7)(C), (b) (6) was sworn in, and it was explained that the Kalkines warning had already been executed. IC (b) (6), (b) (7)(C) read the Kalkines warning for the record.

**Professional Background**

[00:02:30] (b) (7)(C), (b) (6) [redacted]

**May/June 2007**

[00:05:45] When asked how he came to be assigned to the Timberline High School bomb threat investigation, (b) (7)(C), (b) (6) explained that the Lacey PD approached the cybercrime task force in Seattle. Originally, Detective (b) (7)(C), (b) (6) was assigned to be the lead in the investigation, but because his deputization through the Washington State Patrol had lapsed it was decided that (b) (7)(C), (b) (6) would step in as lead. When asked what he meant by "deputization," (b) (7)(C), (b) (6) explained that (b) (7)(C), (b) (6) was detailed to the cybercrime task force from Washington State Patrol, and he was working as a computer forensic examiner and investigator. When it was realized that his deputization had lapsed, (b) (7)(C), (b) (6) was asked to lead. That is why some of the early e-mails were from (b) (7)(C), (b) (6).

| Special Agent Name and Signature: | (b) (7)(C), (b) (6), Program Analyst | Date: 04/07/2015 |
|---|---|---|

When asked who his supervisor was in June 2007, [redacted] named [redacted]. When asked how long he had worked for [redacted] by that point, [redacted] estimated since the beginning of 2007, so approximately five or six months.

[00:07:50] When asked to describe his meeting with Lacey PD, [redacted] explained that Lacey PD came to the Seattle division and met with the investigative team, which consisted of [redacted], Detective [redacted], Intelligence Analyst [redacted], Information and Technology Specialist [redacted], AUSA [redacted], and [redacted].

At the meeting, the investigative team was briefed on the attacks occurring against Timberline High School, including the series of evacuations that had occurred at the school. [redacted] explained that the police department was coming in and sweeping the school for bombs, and when none were found the kids were brought back in. He added that more bomb threats came in so they cleared the school, but then threats came in regarding the Virginia Tech sniper, so they sent the kids home. They knew that the subject was likely familiar with the school given the details in threats he was sending, but it was not known if it was a student, former student, faculty member, or just someone in the district.

[00:09:40] [redacted] was asked if a game plan was decided on during that meeting. He explained that Lacey PD was going to continue to investigate the targets that had been identified during interviews with faculty members, and FBI was going to reach out to Legat Rome to ask for their assistance working the overseas IP addresses that had been used in the attack.

[00:10:40] When asked if he had ever heard of a CIPAV, [redacted] responded yes and explained that it is a tool used to identify the IP address of a machine hiding behind proxies. When asked if the use of a CIPAV was discussed at the meeting with Lacey PD, [redacted] responded that he could not remember if it was discussed then. It came up in the investigation because Seattle was not receiving a response from the Legat offices. [redacted] was asked if it was fair to say that a CIPAV is used to identify an IP address that is being hidden behind one or more proxy IP addresses. [redacted] agreed.

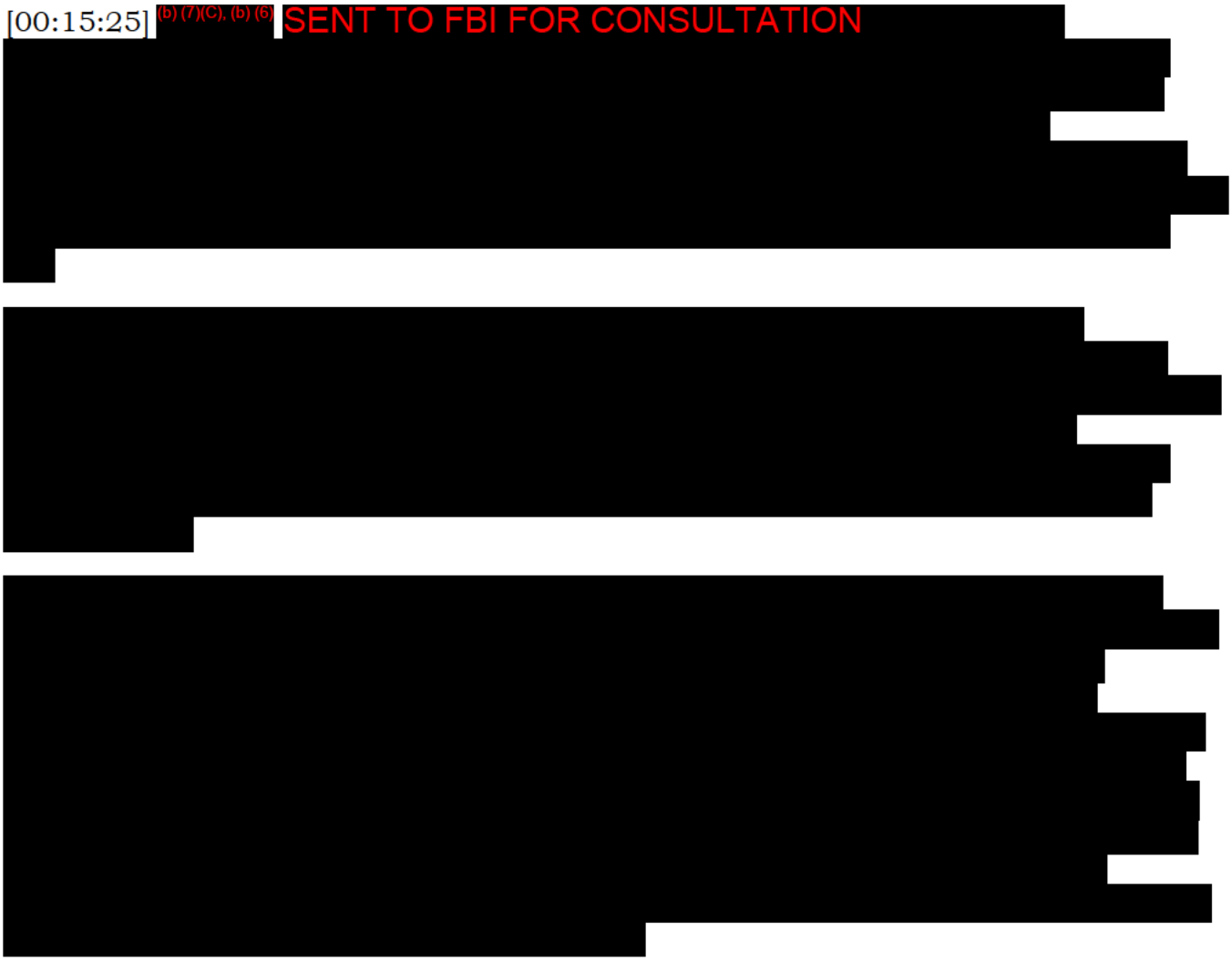
**Internal Approval Levels/Protocols to use a CIPAV**

[00:12:40] [redacted] was asked if, back in 2007, there were certain approvals that FBI had to obtain before a CIPAV could be deployed. [redacted] stated that they needed the approval of the Operation Technology Division at Quantico because the [redacted]
SENT TO FBI FOR CONSULTATION
[redacted]

SENT OT FBI FOR CONSULTATION In addition to those approvals, they would also need to obtain a search warrant, and in some cases apply for a pen register if they needed to.

***AP_000737,*** SENT TO FBI FOR CONSULTATION

[00:15:25] (b) (7)(C), (b) (6) SENT TO FBI FOR CONSULTATION



**Decision to use CIPAV**

[00:19:20] It was pointed out that the FD-759 indicates that they had spoken with AUSA (b) (7)(C), (b) (6) and (b) (7)(C), (b) (6) was asked what the investigative team had discussed with (b) (7)(C), (b) (6) regarding the undercover activity. (b) (7)(C), (b) (6) explained that FBI learned from the Lacey PD that they had identified (b) (7)(C), (b) (6) as potential targets, so FBI executed an emergency pen register on (b) (7)(C), (b) (6) home internet connection. Unfortunately that did not yield any leads related to the Timberline threats.

Upon realizing that the pen register, Lacey PD interviews, and contact with Legat Rome were not going to yield any results, the team contacted Behavioral Science. (b) (7)(C), (b) (6) added that (b) (6), (b) (7)(C) participated on that call, as did a local prosecutor whose name (b) (6), (b) (7)(C) could not recall.

[00:23:20] (b) (7)(C), (b) (6) was directed back to the briefing with behavioral science and asked if his contact was (b) (7)(C), (b) (6) agreed. When asked if (b) (7)(C), (b) (6) discussed the best approach to take with the unknown subject, (b) (7)(C), (b) (6) explained that (b) (7)(C), (b) (6) said they needed to play on the subject's narcissism. Then the topic of using a press angle to exploit the subject's narcissism and bait him into an online dialogue came up as a means of delivering the CIPAV. (b) (7)(C), (b) (6) added that he believed the CIPAV was freely discussed during the behavioral science conversation.

[00:21:20] (b) (7)(C), (b) (6) explained that around this time they also reached out to two program managers at headquarters, SSA (b) (7)(C), (b) (6) and SSA (b) (7)(C), (b) (6) had worked with (b) (7)(C), (b) (6) (b) (6), (b) (7)(C), and knew he had utilized a CIPAV before. (b) (7)(C), (b) (6) put (b) (7)(C), (b) (6) in touch with a CHIPs attorney (b) (6), (b) (7)(C) who utilizes CIPAV, and the Seattle team obtained one of their affidavits to review. When asked what he meant by a CHIPs attorney, (b) (7)(C), (b) (6) explained that CHIPs stood for "Computer Hacking/Intellectual Property," and CHIPs attorneys were congressionally funded and focused on intellectual property or intrusion cases. (b) (7)(C), (b) (6) added that (b) (7)(C), (b) (6) was a CHIPs attorney. The investigative team also spoke with AUSA (b) (6), (b) (7)(C), (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), who had utilized a CIPAV before. After the Seattle team obtained affidavits from (b) (7)(C), (b) (6) and (b) (7)(C), (b) (6), they went down the route of using a CIPAV in the Timberline investigation. (b) (7)(C), (b) (6) added that, at the time, there was a lot of pressure from the high school to resolve the situation, particularly because there were concerns that the person sending the threats was going to ruin the upcoming graduation. Therefore, because they were dealing with threats to life and limb, they were considering the CIPAV option.

[00:24:15] (b) (7)(C), (b) (6) was asked if, during the conversation with (b) (7)(C), (b) (6) about the press angle, there was more detail to the conversation or if it was just limited to the press angle recommendation. (b) (7)(C), (b) (6) stated that he could not recall, and added that he knew they talked about the Associated Press and using a reporter to give more notoriety to the subject, but could not be certain it was during that conversation.

When asked if he recalled whether anyone brought up or considered whether this was a sensitive circumstance during that conversation with BAU, (b) (7)(C), (b) (6) responded not that he could recall. When asked if (b) (7)(C), (b) (6) was present for the conversation with (b) (7)(C), (b) (6) responded yes and added that the whole team, including AUSA (b) (6), (b) (7)(C) was present. When asked if anyone at the meeting raised any concerns about impersonating a reporter, (b) (7)(C), (b) (6) responded no.

**Court Authorization to Deploy CIPAV**

[00:26:05] (b) (7)(C), (b) (6) was asked what role he played in getting court authorization to deploy the CIPAV. He explained that he obtained a draft affidavit from (b) (6), (b) (7)(C) and discussed it with (b) (7)(C), (b) (6), and then tweaked the affidavit for use with the Timberline investigation. Furthermore, since the CIPAV tool belonged to the Operation Technology Division, they wanted their attorney's to review the affidavit to ensure it did not reveal too much about the CIPAV tool. (b) (7)(C), (b) (6) named (b) (7)(C), (b) (6) as one of the attorneys who approved the affidavit before it went to the judge.

(b) (7)(C), (b) (6) was asked if he had seen any of the recent news publications about the Timberline investigation and the methods used, particularly the concern about the affidavit and the fact that it did not detail information about the undercover operation. (b) (7)(C), (b) (6) responded that he has seen the articles. When asked why he did not include any details about the undercover operation in the affidavit, (b) (7)(C), (b) (6) explained that he did not think it was needed for probable cause or securing the court order, and added that (b) (7)(E)

**Division Approval of Undercover Operation**

[00:28:30] (b) (7)(C), (b) (6) was asked if it was his understanding that, because it was an online undercover operation, the team only needed to get approval at the division level. (b) (7)(C), (b) (6) stated that because they believed the operation did not require a sensitive circumstance, it could be approved at the division level. (b) (7)(C), (b) (6) was asked who on the investigative team was responsible for obtaining division approval, and he named (b) (7)(C), (b) (6). He stated that (b) (7)(C), (b) (6) handled all the approvals with ASAC (b) (7)(C), (b) (6) while (b) (7)(C), (b) (6) was focused on the pen register and preparing the affidavit with the AUSA and OTD.

When asked if he had been a part of any briefings given to ASAC (b) (7)(C), (b) (6) by (b) (7)(C), (b) (6) responded no. When asked if he had any responsibilities in determining whether or not a sensitive circumstance existed in this particular investigation, or if that fell to (b) (7)(C), (b) (6) stated that he believed (b) (7)(C), (b) (6) and ASAC (b) (7)(C), (b) (6) would make the ultimate call as to whether a sensitive circumstance existed.

[00:31:10] (b) (7)(C), (b) (6) was read a section of the current guidelines in the Undercover and Sensitive Operations Policy Implementation guide. It was noted that the language is similar to what was in effect in 2007. With regards to privileged relationships and sensitive circumstances, the guide reads: "A significant risk that a third-party might enter into a professional or confidential relationship with a person participating in a UCO who is acting as an attorney, physician, clergyman, or member of the news

media." When asked if he believed that language applied to the situation with the Timberline investigation, (b) (7)(C), (b) (6) responded no, adding that there was not a third-party involved, just the subject and undercover individual. Furthermore, the purpose of connecting with the individual was not to solicit a privileged communication, but to deliver the CIPAV.

(b) (6), (b) (7)(C) was read a section of the Field Guide Undercover and Sensitive Operations, which was in effect in 2007. It was pointed out that there was a note that read: "These sensitive circumstances are listed in order to identify any operational scenario in which privileged communications or defense trial strategy might be overheard, a relationship with a subject is established which the subject believes to be privileged, or a cooperating individual may be placed in an ethical or profession jeopardy because of his or her cooperation with the FBI. It is often the case in these scenarios that these apparent problems never actually materialize, or that if they do measures can be taken to mitigate them. Nevertheless their existence alone is a sensitive matter requiring CUORC review under the AGG." (b) (7)(C), (b) (6) was asked if the note regarding privileged relationships was taken into consideration during the investigation. (b) (7)(C), (b) (6) stated that he did not think it applied at the time. He added that he defaulted to his supervisor (b) (7)(C), (b) (6), who would defer to the AGG-UCO or FGUSO. (b) (7)(C), (b) (6) stated that he did not think he and (b) (7)(C), (b) (6) had in depth discussions about those points, but he remembered (b) (7)(C), (b) (6) reviewing the manuals.

(b) (7)(C), (b) (6) was asked if he thought there was a significant risk that the subject would enter into a professional or confidential relationship with (b) (7)(C), (b) (6) during the course of the operation. (b) (7)(C), (b) (6) responded no, adding that they were limited to three substantial contacts and the purpose was to get the subject to click the link and deploy the CIPAV. He added that once the link was deployed, the undercover operation stopped. Furthermore, the investigative team never met with the subject in person, and did not know any identifying characteristics about him other than he was likely in the western district of Washington.

**Undercover Operation**

(b) (7)(C), (b) (6) was directed to OIG documents ANP_000101-000102 (handwritten notes); ANP000094-000099 (chat exchanges), for his reference.

[00:37:15] (b) (7)(C), (b) (6) was asked when he first made contact with the subject in an undercover capacity. He indicated to ANP_000101 and 000102, and said it looked like they first reached out on the evening of June 12, 2007. When asked if the handwritten notes were his, (b) (7)(C), (b) (6) stated that everything from June 12 were his notes, and then it looked like another individual picked up the notes on June 13.

[00:38:40] When asked how he reached out to the subject on June 12, 2007, (b) (7)(C), (b) (6) stated that he believed it was through a Myspace private message that included a

link to the CIPAV. (b) (7)(C), (b) (6) added that they thought that simply mentioning the article would be enough to get the subject to click on the link, and the communication would end there. When asked if the subject responded to that initial message, (b) (7)(C), (b) (6) responded no and added that he sent a second e-mail either that evening or the next day, June 13, 2007.

(b) (7)(C), (b) (6) counsel, (b) (7)(C), (b) (6) indicated to the chat conversation listed in ANP000096 and pointed out that because the Myspace page was public, and the subject was willing to disclose his comments to the public, the subject likely did not intend the conversation with the undercover to be confidential. [**OIG Note:** I believe ANP000096 (b) (6), (b) (7)(C) is referring to is the Gmail Chat between (b) (6), (b) (7)(C) and the subject, not the general Myspace account]. (b) (7)(C), (b) (6) pointed out that if the subject was willing to blast his comments over a public web site, he would not have considered their conversation to be confidential.

***ANP000097-000098***

[00:42:50] (b) (7)(C), (b) (6) attention was directed to the message he sent the subject's Myspace inbox on June 13, 2007 at 2:51 PM. (b) (7)(C), (b) (6) explained that this message was a follow-up to the message that contained the CIPAV link the subject did not click. The follow-up message essentially stated that they were disappointed they did not get a response from the subject, and then included the link to the CIPAV.
(b) (7)(C), (b) (6), (b) (7)(E)

[00:45:00] It was pointed out that the subject responded to the 2:51PM message by telling (b) (7)(C), (b) (6) to leave him alone. (b) (7)(C), (b) (6) then responded at 3:21 PM with: "I respect that you do not want to be bothered by the Press. Please let me explain my actions. I am not trying to find out your true identity. As a member of the Press, I would rather not know who you are as writers are not allowed to reveal their sources. The school has continually requested that the Press NOT cover this story. After the School Meeting last night, it is obvious to me that this needs coverage. Readers find this type of story fascinating. People don't understand your actions and we are left to guess what message you are trying to send."

(b) (7)(C), (b) (6) was asked what response he hoped his 3:21PM message would elicit from the subject. (b) (7)(C), (b) (6) explained that all they needed the subject to do was to click the link to deploy the CIPAV. When asked if he crafted the 3:21 response himself, of if there was anyone else involved, (b) (7)(C), (b) (6) responded that the entire investigative team was standing around him while he made contact, and there was a lot of consulting

about what to say. Every response was carefully considered by the team before it was sent.

[00:47:00] It was pointed out that the subject then asked how he could help, and at 3:24PM (b) (7)(C), (b) (6) responded by asking if the article and pictures were accurate. When asked what the purpose was of this message, (b) (7)(C), (b) (6) explained that he believed the (b) (7)(E) (b) (7)(E) The investigative team contacted OTD and they reviewed the results, and were able to identify the problem. OTD informed the team that (b) (7)(E) that contained a CIPAV, so the team devised the plan to send pictures to the subject for approval.

(b) (7)(C), (b) (6) added that there was one clarification he wanted to make to the media articles reporting that the FBI put thousands of people at risk because the CIPAV could capture information from everyone. Sanders explained that the CIPAV was (b) (7)(E) They sent that CIPAV to the subject and asked him to pick the pictures he wanted, the CIPAV successfully deployed and captured the information needed to break through the proxies being used, and identified the Comcast IP address in Lacey, Washington. Lacey PD used exigent circumstances with Comcast to identify the subscriber, and then execute a search warrant within hours.

[00:49:45] (b) (7)(C), (b) (6) was asked if, while they were crafting the e-mails to the subject, anyone brought up any concerns about whether the operation would trigger a sensitive circumstance. He responded that he did not recall sensitive circumstances coming up during those conversations.

With regard to online communications and the three substantive contacts in 2007, (b) (7)(C), (b) (6) was asked how the number of contacts was quantified when dealing with electronic communications like e-mail and instant messaging. (b) (7)(C), (b) (6) explained that it was explained to them in their online uncover training courses that a back-and-forth chat was a contact until that chat stopped. An e-mail conversation going back-and-forth over a matter of days, however, could also be considered just one conversation. Therefore, a conversation occurring over a reasonable amount of time could be considered one contact, even if it spanned more than a day.

[00:51:30] (b) (7)(C), (b) (6) was read an excerpt from the Attorney General Guidelines, which were updated in 2003 [ANP001436]: "In the context of online communications such as e-mail and internet relay chat, multiple transmissions or e-mail messages can

constitute one contact, much like a series of verbal exchanges can comprise a single conversation. Factors to be considered when determining whether multiple online transmissions constitute a single contact or multiple contacts, include the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged, i.e. e-mail versus IRC." When asked if that sounded like his interpretation of the guidelines surrounding number of online contacts, (b) (7)(C), (b) (6) responded yes and added that even when the subject asked to switch from Myspace messages to Gmail chat, it was still the same conversation and therefore same contact. The method of communicating that conversation just changed formats.

[00:54:25] (b) (7)(C), (b) (6) attention was directed to the Situation Action Background (SAB) dated October 31, 2014 [ANP000823]. When asked if he played any role in drafting the SAB, (b) (7)(C), (b) (6) stated that he drafted bullet points that cyber division program managers used to draft the SAB. The Cyber Law unit then reviewed the SAB. When asked if he played any role in the section of the SAB dealing with policies or legal analyses, (b) (7)(C), (b) (6) responded no.

**Record Ends**

UNITED STATES DEPARTMENT OF JUSTICE

OFFICE OF THE INSPECTOR GENERAL

----------X

IN RE: :

INTERVIEW OF (b) (7)(C), (b) (6) :

----------X

Wednesday, December 15, 2015

Washington, D.C.

Telephonic Interview of

(b) (6), (b) (7)(C)

By the U.S. Department of Justice, Office of the Inspector General before:

FOR THE OFFICE OF THE INSPECTOR GENERAL:

(b) (7)(C), (b) (6), Oversight and Review Division

(b) (7)(C), (b) (6), Oversight and Review Division

I N D E X

EXHIBITS

| EXHIBIT NUMBER | PAGE NUMBER |
| --- | --- |
| None | |

P R O C E E D I N G S

(b) (7)(C), (b) (6): Today is December 16, 2015 and we are on the phone with, you are (b) (7)(C), (b) (6), right (b) (7)(C), (b) (6)?

(b) (7)(C), (b) (6): No, that's not correct. I'm (b) (7)(C), (b) (6) (b) (7)(C), (b) (6) so I'm a Supervisory Special Agent.

(b) (7)(C), (b) (6): Okay, Supervisory Special Agent (b) (7)(C), (b) (6). Also present is Special Agent (b) (7)(C), (b) (6) of the OIG and myself, (b) (7)(C), (b) (6), an investigative counsel with the OIG.

(b) (7)(C), (b) (6), as I said off the record, we are here to just talk about this 2007 case involving a student at Timberline High School near Seattle, Washington who actually has since been convicted, of making bomb threats against the high school through the internet.

So before we get started, do you swear to tell the truth, the whole truth and nothing but the truth?

(b) (7)(C), (b) (6) I do.

(b) (7)(C), (b) (6): All right, so let's start with the easy stuff first. Can you give me sort of the (b) (7)(C), (b) (6) 101; how long you've been with the FBI and sort of take me through your career?

(b) (7)(C), (b) (6): Of course. So I joined the FBI in (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (7)(C), (b) (6)
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
(b) (7)(C), (b) (6)
(b) (7)(C), (b) (6)
(b) (7)(C), (b) (6)
(b) (7)(C), (b) (6)
(b) (7)(C), (b) (6).

(b) (7)(C), (b) (6): Okay, I want to take you back to May 2007. In that time period, do you recall working on a case involving an individual named (b) (7)(C), (b) (6)?

(b) (7)(C), (b) (6): I do. I have notes here and e-mails to refresh my memory, but I do have recollection of working that case, yes.

(b) (7)(C), (b) (6): What was your role in that particular investigation?

(b) (7)(C), (b) (6): So I was the BAU's (b) (6), (b) (7)(C) SSA that was assigned to this case. There was a request that had come in from the Seattle office to provide assistance on this bomb threat case and that's traditional. The BAU operates really

in a consultant capacity where if a field office requests assistance, we will provide insights, observations and recommendations.

(b) (7)(C), (b) (6): Okay. And what were you asked to do?

(b) (7)(C), (b) (6) Asked to provide really a threat assessment first, you know just something that does the threat in there represent a real and credible threat to the safety of the staff and the students at Timberline High School and then the second request was to develop a strategy to entice the offender into clicking on a link that would deploy a CIPAV, which (b) (6), (b) (7)(C) this case, (b) (7)(C), (b) (6) is the "Computer Internet Protocol Address Verifier."

(b) (7)(C), (b) (6) Okay, and I want to talk to you about that second component, the advice to get the, I guess the perpetrator if you will, to click on this link. What advice, if any, did you give?

(b) (7)(C), (b) (6) So in looking at the language and the verbiage and the delivery methods and the, I believe the creation of the MySpace page and just the behavior of the offenders, the team and I, and by the way, so (b) (7)(C), (b) (6) at BAU, we really don't do anything alone per se as a general course of operations. So you know the other I think four or five SSAs and I brought in to assist on this case.

Now what we observed in looking at the offender's behavior and his language or his or her language, was that it appeared to be very narcissistic, very attention seeking, that this was a person who was feeding off of the attention that he or she was getting as a result of the bomb threats. So specifically, we thought that narcissism would override any kind of caution or vigilance or suspicion that the offender might have if presented with a, you know click-on-a-link kind of scenario in an e-mail. And so we opined and recommended that use that narcissism, use the offender's narcissism to override his suspicions on clicking on the link. And one way to do that would be to say that if he thought that he was clicking on some type of story or media report about him, that that would appeal to his narcissism.

(b) (7)(C), (b) (6) Okay, so is it fair to say then your advice was to take, I guess, like almost a reporter approach?

(b) (7)(C), (b) (6) So I don't remember exactly how it went from you know saying to click on the link to a story about yourself, to having the sender of the e-mail portray a reporter.

I have from my notes that we had a conference call on June 11th and I don't have any specific, I don't know if you have a copy of my notes.

(b) (7)(C), (b) (6) I do not, but who was present for

that conference call?

(b) (7)(C), (b) (6) So present in that conference call was obviously myself on the BAU side, Supervisory Special Agents (b) (7)(C), (b) (6) (b) (7)(C), (b) (6) and (b) (7)(C), (b) (6). And then I have in my notes reflecting on the call from Seattle was SSA (b) (6), (b) (7)(C). I have a reference (b) (7)(C), (b) (6) here which I assume is (b) (7)(C), (b) (6). Someone named (b) (7)(C), (b) (6) and (b) (7)(C), (b) (6).

(b) (7)(C), (b) (6) Anybody else?

(b) (7)(C), (b) (6) I do have a note here that says Lieutenant (b) (6), (b) (7)(C) with numbers as well, so perhaps maybe Lieutenant (b) (6), (b) (7)(C) was part of that too.

(b) (7)(C), (b) (6) Okay, any reference to an Assistant U.S. Attorney names (b) (6), (b) (7)(C)?

(b) (7)(C), (b) (6) I do not see that anywhere in my notes, no.

(b) (7)(C), (b) (6) Okay, just curious. But you did suggest using a media approach, is that fair?

(b) (7)(C), (b) (6) Yeah, again using something that was, again would appeal to his narcissism and if he thought that he was reading a report or some type of article or something about himself, that that would override his suspicions. And again, I don’t recall if it was you know during that consult that the discussion said, well who would the sender be? I

do, I don't have any recollection of ever saying specifically you know this should be a reporter from a certain agency, but.

(b) (7)(C), (b) (6) Um-hmm. Is that sort of implied though if you are going to use like an article?

(b) (7)(C), (b) (6) I wouldn't, no I don't know that I would said it is implied. I suppose it could be a freelance journalist, but.

(b) (7)(C), (b) (6) Okay, but regardless, not necessarily a reporter from like a nationally renowned newspaper like a freelance journalist, but there is sort of an implication that the person who is sending the email has written a story about this particular individual.

(b) (7)(C), (b) (6) Yeah, and again I don't remember specifically how that, the discussion about who the sender would be, --

(b) (6), (b) (7)(C) Um-hmm.

(b) (6), (b) (7)(C) -- I just again remember that it was, you know saying if this was a media article about that person or about the offender, that he would feel compelled to look at it.

(b) (6), (b) (7)(C) Okay, fair enough. All right, is there anything else about this particular case that you think we need to be aware of?

(b) (6), (b) (7)(C) No, that was, I mean I think again

just understanding the basic framework I would say would be that when the BAU provides any kind of recommendations, it's never, in my experience it's never been where the BAU provides any kind of guidance as to whether or not you know that's, there's authorization from our side. In other words, we don't bring in our Chief Division Counsel on the strategy recommendations to say, hey is this you know and moving forward is this something where you have appropriate authorization.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C) That authorization is assumed that the receiving office goes through that process.

(b) (6), (b) (7)(C) Okay, fair enough. The only thing I'd ask, can you send me a .pdf copy of your handwritten notes of that meeting?

(b) (6), (b) (7)(C) Of course.

(b) (6), (b) (7)(C) And then did you guys do any internal write up about this?

(b) (6), (b) (7)(C) We did not.

(b) (6), (b) (7)(C) Okay. Yeah, if you could send me a copy of those notes, that would be great.

(b) (6), (b) (7)(C) I would be happy to.

(b) (6), (b) (7)(C) All right. With that, I think we can go off. Do you have any questions (b) (6), (b) (7)(C)?

(b) (6), (b) (7)(C) No.

(b) (6), (b) (7)(C) We can go off the record and that's all we have.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C) All right, thank you [redacted].

(b) (6), (b) (7)(C) You bet [redacted]. Thank you. Thanks [redacted].

(b) (6), (b) (7)(C) Bye now.

(b) (6), (b) (7)(C) All right, thanks [redacted].

(b) (6), (b) (7)(C) Nothing follows.

[WHEREUPON, THE INTERVIEW WAS CONCLUDED.]

# C E R T I F I C A T E

I hereby certify that the foregoing pages represent an accurate transcript of the electronic sound recording of the proceedings before the Department of Justice, Office of Inspector General in the matter of:

Interview of (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

Department of Justice
Office of the Inspector General
Oversight and Review Division

December 16, 2015

UNITED STATES DEPARTMENT OF JUSTICE

OFFICE OF THE INSPECTOR GENERAL

----------X

IN RE: :

INTERVIEW OF (b) (6), (b) (7)(C) :

----------X

Thursday, December 17, 2015

Washington, D.C.

Telephonic Interview of

(b) (6), (b) (7)(C)

By the U.S. Department of Justice, Office of the Inspector General beginning at ____ before:

FOR THE OFFICE OF THE INSPECTOR GENERAL:

(b) (6), (b) (7)(C), Oversight and Review Division

(b) (6), (b) (7)(C), Oversight and Review Division

I N D E X

EXHIBITS

| EXHIBIT NUMBER | PAGE NUMBER |
| --- | --- |
| None | |

P R O C E E D I N G S

(b) (6), (b) (7)(C): Today is Thursday, December 17, 2015. We are on the phone with (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Assistant United States Attorney in the Western District of Washington, correct?

(b) (6), (b) (7)(C): Correct.

(b) (6), (b) (7)(C): And also present is (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), a Program Analyst with the OIG and myself, (b) (6), (b) (7)(C), an Investigate Counsel with the OIG.

(b) (6), (b) (7)(C), to start off, do you swear to tell the truth, the whole truth and nothing but the truth?

(b) (6), (b) (7)(C): I do.

(b) (6), (b) (7)(C): Excellent. As we discussed off the record, I am interviewing you today regarding the FBI's investigation of some bomb threats that occurred in May 2007 involving Timberline High School.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C): But before we get there, I was just curious. Could you just take me through your career at the U.S. Attorney's Office?

(b) (6), (b) (7)(C) Gosh, I wasn't prepared to do that.

(b) (6), (b) (7)(C): I'm so sorry.

(b) (6), (b) (7)(C): I can put it in a nutshell. (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) .

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C): Oh wow.

(b) (6), (b) (7)(C) (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C): Okay. No that was helpful. I was just curious about your background.

Drawing your attention to May 2007, did you come to be involved in an FBI investigation involving bomb threats against Timberline High School?

(b) (6), (b) (7)(C) Yes.

(b) (6), (b) (7)(C): How did you come to be involved in that investigation?

(b) (6), (b) (7)(C) Well to the best of my recollection, --

(b) (6), (b) (7)(C): Sure.

(b) (6), (b) (7)(C) -- it was on request from the FBI to become involved and to, the focus became working up a warrant to use in the case to try and identify the perpetrator.

(b) (6), (b) (7)(C): Okay. And so sort of it sounds like the FBI specifically requested your assistance?

(b) (6), (b) (7)(C) Well I, yes, I would say so. I mean I was the primary, probably the primary, maybe the only cyber attorney at that point in time. I'm not sure.

(b) (6), (b) (7)(C): Okay. And as the attorney who was going to work with the FBI, what were your roles and responsibilities going to be?

(b) (6), (b) (7)(C) Again with regard to this case in particular, I think very quickly it became preparing or working with Agent (b) (6), (b) (7)(C) to prepare a warrant in order to use the tool, the CIPAV tool --

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) -- in order to try and identify the perpetrator.

(b) (6), (b) (7)(C): Okay. And by Agent (b) (6), (b) (7)(C), you are talking about (b) (6), (b) (7)(C)?

(b) (6), (b) (7)(C) Yes.

(b) (6), (b) (7)(C): Okay. So in regard to the search warrant, what did you draft in relation to that document?

(b) (6), (b) (7)(C) Boy, I can't give you any detail on that at this point.

(b) (6), (b) (7)(C): Okay. Would you or, and maybe past practice can help out here, would you have drafted the affidavit or would that have been something that (b) (6), (b) (7)(C) would have done?

(b) (6), (b) (7)(C) Probably, typically the agents did the

drafting of the affidavits and after the first draft there would be interaction with us going back and forth to answer questions of support in certain areas as probable case is lacking or whatever.

(b) (6), (b) (7)(C): Okay. And so you would have been actually reviewing his affidavit as he was drafting it, sort of making comments?

(b) (6), (b) (7)(C) Correct.

(b) (6), (b) (7)(C): Okay. And in regard just to sort of give you some background, the question I wanted to ask is the affidavit which we've had a chance to review which I couldn't send to you because of internal rules, --

(b) (6), (b) (7)(C) Yes.

(b) (6), (b) (7)(C): -- but the affidavit to the warrant discusses specifically the use of the CIPAV, what the CIPAV's capabilities are, how it's going to be used, but what's not discussed in the affidavit is the ruse or the technique by which, sort of the details if you will, of how the FBI is going to get the unknown subject --

(b) (6), (b) (7)(C) Right.

(b) (6), (b) (7)(C): -- to activate it. And the question I had is would that be something that would be normally included in an affidavit, sort of the how they are going to get him to activate it part or is that something that's unnecessary?

(b) (6), (b) (7)(C) I'd say typically that's unnecessary, I mean I don't recall any warrant that involved a discussion of how it would be affected.

(b) (6), (b) (7)(C): I see. Okay, so you wouldn't discuss sort of the, necessarily how the operation is going to play out, you would just discuss the actual tool itself and how it works?

(b) (6), (b) (7)(C) Right, well that, I think, I believe that's the only warrant I've ever been involved with on a CIPAV.

(b) (6), (b) (7)(C): Oh okay. All right. And so in regard to the CIPAV, did you discuss using the CIPAV with your supervisor?

(b) (6), (b) (7)(C) I would assume I did.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) I don't recollect conversations about it.

(b) (6), (b) (7)(C): All right. And in regard to deploying the CIPAV, did the FBI, either (b) (6), (b) (7)(C) or (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), discuss with you their plan on how they planned on getting it deployed?

(b) (6), (b) (7)(C) I don't recall any conversations specifically about that, no.

(b) (6), (b) (7)(C): Is that something that they would normally discuss with you?

(b) (6), (b) (7)(C) Uh, no.

(b) (6), (b) (7)(C): Okay. So they wouldn't share the details of the actual operation with you, just the tool that they planned on using?

(b) (6), (b) (7)(C) Right. Well most typically we'd be working with search warrants. This was an unusual case, but protocol generally would, I mean almost, I mean always, they don't discuss, right, how they are going to effectuate the warrant or the process.

(b) (6), (b) (7)(C): Okay. And you mentioned the word protocol there, what do you mean by that?

(b) (6), (b) (7)(C) And I don't think they're, use of that word didn't mean to suggest there was a, there is a formal or written protocol, it's just an operating SOP or the way things were done.

(b) (6), (b) (7)(C): Okay. All right. Did you, to your recollection, and some of these questions I apologize if they seem repetitive; I'm trying to answer a couple of other people's questions at the same time.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): Did you ask or inquire as to how they planned to deploy the CIPAV?

(b) (6), (b) (7)(C) No I don't recall doing that.

(b) (6), (b) (7)(C): Okay. Would you, I'm going to ask this question in two parts. Did you have any responsibility

to approve that plan on how they were going to deploy the CIPAV?

(b) (6), (b) (7)(C) No.

(b) (6), (b) (7)(C): Okay. That's not a responsibility that you, would that have been a responsibility you would have had?

(b) (6), (b) (7)(C) No.

(b) (6), (b) (7)(C): Okay. That's something that's done internally in the FBI, correct?

(b) (6), (b) (7)(C) Yes.

(b) (6), (b) (7)(C): I'm sorry, can you repeat that?

(b) (6), (b) (7)(C) I would believe so, yes. I don't know what the internal processes of the FBI are.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) I mean I know that it was standard procedure for Agent (b) (6), (b) (7)(C) to work with Headquarters on I believe almost everything that he did that I worked with him on which would be cyber matters, he referred to Headquarters repeatedly in interactions with them.

(b) (6), (b) (7)(C): And how do you know that?

(b) (6), (b) (7)(C) Oh he said that. I don't know, I mean, I don't think he was lying to me about that, but -.

(b) (6), (b) (7)(C): Yeah, and I wasn't trying to imply that, I just wanted to know what the basis of your knowledge was for that.

(b) (6), (b) (7)(C) The comments by him and I think, again I worked with Agent (b) (6), (b) (7)(C) on a number of cases and some very big cases and he was a guy who was constantly concerned about compliance with FBI policies and rules. He referred to them many times. He referred many times throughout these cases to interact with people from Headquarters because they were high profile cases.

(b) (6), (b) (7)(C): Okay. At some point we know that Agent (b) (6), (b) (7)(C) consulted with a Behavioral Assessment Unit at Quantico.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): Were you aware that he had done that?

(b) (6), (b) (7)(C) You know I thought perhaps that he had mentioned something about that and I'm not sure of that memory.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) But I think that he might have mentioned that.

(b) (6), (b) (7)(C): And I'm going to try, maybe I can jog a memory just through the question.

(b) (6), (b) (7)(C) Um-hmm.

(b) (6), (b) (7)(C): Did he have any discussions with you about the advice they may have given about taking a media approach to deploy the CIPAV?

(b) (6), (b) (7)(C) Again, he, there might have been some discussion of that. I don't remember that clearly.

(b) (6), (b) (7)(C): Okay. All right. And I'll ask this question as well in relations to the BAU. Do you recall if you ever participated in a conference call with the Behavioral Assessment Unit Special Agent?

(b) (6), (b) (7)(C) No, I don't recall that.

(b) (6), (b) (7)(C): Okay. All right. Now our understanding is that in order to effectuate the deployment of the CIPAV, the FBI planned on communicating with the unknown subject through an e-mail. Was that something that you were aware of?

(b) (6), (b) (7)(C) I might have been aware of it. I don't recall. If we wrote it up in the affidavit, I don't recall.

(b) (6), (b) (7)(C): Okay. Well then my next question would be did you see any e-mails in advance that they used to effectuate that deployment of the CIPIV?

(b) (6), (b) (7)(C) I don't recall.

(b) (6), (b) (7)(C): Okay. Is it something that you would normally see as an AUSA?

(b) (6), (b) (7)(C) I don't think so.

(b) (6), (b) (7)(C): You don't think so?

(b) (6), (b) (7)(C) No.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) I mean again this is the only CIPAV

warrant I ever worked on that I recall, so in the course of all the other warrants I worked on, I don't recall ever seeing an e-mail that would, because, well they wouldn't have involved an e-mail generally.

(b) (6), (b) (7)(C): Okay. And again this gets back to I guess that basic question of you weren't involved in sort of the operational aspect of the FBI's plans in general?

(b) (6), (b) (7)(C) Correct.

(b) (6), (b) (7)(C): Okay. Did (b) (6), (b) (7)(C) or the FBI agents who were involved in the case, it's (b) (6), (b) (7)(C) and then I think a guy named (b) (6), (b) (7)(C) who was a task force officer, did they need any kind of approval from you to actually engage in their plan?

(b) (6), (b) (7)(C) Not that I, no I don't believe so. Not that I'm aware of.

(b) (6), (b) (7)(C): Okay. I'm just going to take a quick look at something. I'm just going to ask some very specific questions that a colleague of mine asked to ask you.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): They might be repetitive of what we just asked. I just want to go down the list for him.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): Did you review or approve the FBI's planned ruse to impersonate a journalist?

(b) (6), (b) (7)(C) No.

(b) (6), (b) (7)(C): Did they tell you anything about a plan to impersonate a journalist?

(b) (6), (b) (7)(C) Not that I recall.

(b) (6), (b) (7)(C): Okay. We talked about that. We covered that one and we covered that.

All right. Kathryn, I think those are all the questions that I had.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): That moved a lot more quickly than I expected it would.

(b) (6), (b) (7)(C) Okay. Well I would just like to reiterate, I thought (b) (6), (b) (7)(C) was an outstanding agent. He was always diligent, always thorough and always very concerned about complying with the law and policies in every way. He would be the last guy to want to do some kind of lone wolf you know thing under the radar.

(b) (6), (b) (7)(C): Sure.

(b) (6), (b) (7)(C) I mean that's not the way he ever operated.

(b) (6), (b) (7)(C): Okay.

(b) (6), (b) (7)(C) He was in my view, and he is, an outstanding agent and a credit to the FBI.

(b) (6), (b) (7)(C): And I really appreciate that commentary very much.

I just want to make sure if it would be fair for me

to say this. That your role in the FBI's Op, in this investigation was basically to draft the search warrant, right?

(b) (6), (b) (7)(C) Right, to work with him to draft the search warrant. To make sure it would be comprehensible by the judge who was reviewing it and meet any legal requirements necessary.

(b) (6), (b) (7)(C): To pass muster with the court?

(b) (6), (b) (7)(C) Correct.

(b) (6), (b) (7)(C): Excellent. You summed it up better than I ever could have.

And then in regards specifically to the FBI operation, would it be fair to say, that as an AUSA, you had no responsibilities over what the FBI did to effectuate the deployment of the CIPAV?

(b) (6), (b) (7)(C) Yes, I think that's right.

(b) (6), (b) (7)(C): Excellent. I don't have any additional questions and with that I think we can go off the record.

(b) (6), (b) (7)(C) Okay.

(b) (6), (b) (7)(C): Let me just shut this off. Nothing follows.

[WHEREUPON, THE INTERVIEW WAS CONCLUDED.]

# C E R T I F I C A T E

I hereby certify that the foregoing pages represent an accurate transcript of the electronic sound recording of the proceedings before the Department of Justice, Office of Inspector General in the matter of:

Interview of (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)
t
Department of Justice
Office of the Inspector General
Oversight and Review Division

December 22, 2015