Office of the Inspector General
U.S. Department of Justice

A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation

Revised September 2016

EXECUTIVE SUMMARY

Over the course of 1 week in June 2007, a 15-year old high school student e-mailed a series of bomb threats to administrators and staff at Timberline High School, near Seattle, Washington. The threats caused daily school evacuations. The individual used "proxy servers" to e-mail the bomb threats in order to hide his location. When local law enforcement officials were unable to identify or locate the individual, they requested assistance from a cybercrime task force supervised by the Federal Bureau of Investigation's (FBI) Seattle Field Division.

FBI agents on the task force, working with FBI technology and behavioral experts at Headquarters (FBIHQ), developed a plan to surreptitiously insert a computer program into the individual's computer that would identify his location. An FBI undercover agent posed as an editor for the Associated Press (AP) and attempted to contact the individual through e-mail. During subsequent online communications, the undercover agent sent the individual links to a fake news article and photographs that had the computer program concealed within them. The individual activated the computer program when he clicked on the link to the photographs, thereby revealing his location to the FBI. FBI and local law enforcement agents subsequently arrested the individual and he confessed to e-mailing the bomb threats.

The FBI did not publicize the assistance its agents provided local law enforcement. However, on July 18, 2007, 2 days after the individual pleaded guilty, an online technology news website published an article that detailed the method by which the FBI identified the individual. Seven years later, in October 2014, *The Seattle Times* published an article that disclosed the fact that an FBI employee posed as a member of the news media when it contacted and then identified the subject as the author of the bomb threats. Later that same month the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's impersonation of a member of the news media in connection with the FBI's investigation of the bomb threats. In addition, several newspapers wrote articles questioning the tactics the FBI used to identify and arrest the subject who sent the threats.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's actions. In particular, Comey stated that the "technique [the FBI used to identify and apprehend the individual who sent the threats] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

That same day, the Reporters Committee for Freedom of the Press, on behalf of 25 other news organizations, wrote a letter to Comey and Holder voicing its objection to the practice of FBI agents impersonating journalists, saying the practice endangers the media's credibility and undermines its independence, and that it appeared to violate FBI guidelines for when such tactics were permissible.

We initiated this review to examine whether under Department of Justice and FBI policies in effect at the time of the 2007 investigation, agents obtained the appropriate approval for the undercover activities the FBI conducted to locate the individual e-mailing the bomb threats. We also examined whether the undercover activities in 2007 would require a higher level of approval if conducted today under current Department and FBI polices.

As described in our full report, we concluded that FBI policies in 2007 did not expressly address the tactic of agents impersonating journalists. We further found that the FBI's undercover policies then in effect provided some relevant guidance, but were less than clear. As a result, we believe that the judgments agents made about aspects of the planned undercover activity in 2007 to pose as an editor for the AP did not violate the undercover policies in place at the time. We also determined that once the undercover plan was launched, certain investigative decisions were made concerning communications the undercover agent sent to the individual suspected of making the bomb threats that could have increased the level of approval required under FBI policy, a possibility the investigative team did not appear to fully consider.

As we were finalizing this report, the FBI adopted a new interim policy in June 2016 that provides guidance to FBI employees regarding their impersonation of members of the news media during undercover activity or an undercover operation (defined as a series of related undercover activities over a period of time). We found that prior to the adoption of this new interim policy, FBI policy would not have prohibited FBI employees from engaging in the undercover activities agents conducted during the 2007 Timberline investigation. The new interim policy, however, clearly prohibits FBI employees from engaging in undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized as part of an undercover operation. In order for such an operation to be authorized, an application must first be approved by the head of the FBI field office submitting the application to FBIHQ, reviewed by the Undercover Review Committee at FBIHQ, and approved by the Deputy Director, after consultation with the Deputy Attorney General.

We believe the FBI's new interim policy is a significant improvement to policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June 2016. The new interim policy also is an important extension of policies the Department of Justice has previously implemented to regulate certain law enforcement activities that affect members of the news media, such as obtaining information from or about members of the news media in criminal and civil investigations. The FBI should move expeditiously to update its undercover policy guide to incorporate this new interim policy, and widely inform and educate FBI employees about the policy's existence and application.

Based upon our review, we made three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurred with the recommendations.

TABLE OF CONTENTS

I. Introduction

On Sunday, June 3, 2007 an unknown subject, later identified by the Federal Bureau of Investigation (FBI) as 15-year old high school student Charles Jenkins, sent an e-mail containing a bomb threat to numerous teachers and administrators of Timberline High School, near Seattle, Washington.[1] The high school was evacuated the next day. Jenkins e-mailed bomb threats to the school every day of the next week, causing daily evacuations.

Jenkins used "proxy servers" located in Europe to send his e-mails in a manner that would hide his true location. As a result, local law enforcement officials were not able to identify or locate Jenkins and they requested assistance from the Northwest Cybercrime Task Force, which was supervised by the FBI's Seattle Division. The FBI immediately opened an investigation.

FBI agents developed a plan to surreptitiously insert a computer program into Jenkins's computer that would identify his true location. An FBI undercover agent posed as an editor for the Associated Press (AP) and contacted Jenkins through e-mail. During subsequent online communications, the undercover agent sent Jenkins links to a fake news article and photographs that had the computer program embedded within them. Jenkins activated the computer program when he clicked on the link to the photographs, thereby revealing Jenkins's true location to the FBI.

FBI and local law enforcement agents subsequently arrested Jenkins and he confessed to e-mailing the bomb threats. On July 16, 2007 Jenkins pleaded guilty as a juvenile to several state felony offenses and was sentenced to 90 days of juvenile detention, 2 years of supervised release, 2 years of mental health counseling, and 2 years of probation with restrictions on internet and computer usage. Jenkins was also expelled from school.

The FBI did not publicize the assistance its agents provided local law enforcement. However, on July 18, 2007, 2 days after Jenkins pleaded guilty, the online technology news website Wired.Com released an article entitled "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" that detailed the method by which the FBI identified Jenkins. Seven years later, on October 27, 2014, *The Seattle Times* released an article based upon e-mails obtained by the Electronic Frontier Foundation through a Freedom of Information Act request to the FBI. Those e-mails disclosed the fact that the FBI posed as a member of the news media when it contacted and then identified Jenkins as the author of the bomb threats.

On October 30, 2014, the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's impersonation of a member of the news media in connection with its investigation of the bomb threats. In addition, several

[1] Charles Jenkins is a pseudonym.

newspapers wrote articles questioning the tactics the FBI used to identify and arrest Jenkins.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's actions. In particular, Comey stated that the "technique [the FBI used to identify and apprehend Jenkins] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

The same day, the Reporters Committee for Freedom of the Press (RCFP), on behalf of 25 other news organizations, wrote a letter to Comey and then-Attorney General Eric Holder voicing its objection to the practice of FBI agents impersonating journalists, saying the practice endangers the media's credibility and undermines its independence, and that it appeared to violate FBI guidelines for when such tactics are permissible.[2]

We initiated this review to examine whether under Department of Justice (DOJ or Department) and FBI policies in effect at the time of the 2007 investigation, agents obtained the appropriate approval for the undercover activities the FBI conducted to locate Jenkins. We also examined whether the undercover activities in 2007 would require a higher level of approval if conducted today under current Department and FBI polices.

We concluded that FBI policies in 2007 did not expressly address the tactic of agents impersonating journalists. We further found that the FBI's undercover policies then in effect provided some guidance, but were less than clear. As a result, we believe that the judgments agents made about aspects of the planned undercover activity in 2007 did not violate the undercover policies in place at the time. We also determined that once the undercover plan was launched, certain investigative decisions were made that could have increased the level of approval required, a possibility the investigative team did not appear to fully consider.

On June 8, 2016, as we were finalizing this report, the FBI adopted a new interim policy that provides guidance to FBI employees regarding their impersonation of members of the news media during undercover activity or an undercover operation (defined as a series of related undercover activities over a period of time). Under this new policy, FBI agents may only represent, pose, or claim to be members of the news media when authorized by the FBI Deputy

[2] The RCFP also urged the FBI to publicly disclose when and under what circumstances they have digitally impersonated the news media in the past. The RCFP and the AP also filed a request for such records under the Freedom of Information Act (FOIA). When no records were provided, on August 27, 2015, the two media organizations filed a civil action against the FBI and Department of Justice under FOIA seeking an order requiring the agencies to comply with the FOIA request. The FBI subsequently released responsive documents to RCFP and AP in February and March 2016. In the still ongoing litigation, RCFP and the AP are seeking release of the documents the FBI withheld from disclosure pursuant to certain FOIA exemptions.

Director, after consultation with the Deputy Attorney General, as part of an undercover operation reviewed by the Undercover Review Committee (UCRC). The policy expressly prohibits FBI employees from engaging in such activity if it is not part of an undercover operation. Therefore, the undercover activities in 2007 would be prohibited today unless they were part of an undercover operation reviewed by the UCRC and authorized by the FBI Deputy Director, after consultation with the Deputy Attorney General.[3]

Based upon our review, we made three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurred with the recommendations.

II. Methodology of the OIG's Review and Organization of Report

In undertaking this review, the OIG examined approximately 2000 documents, including the FBI's investigative case file, applicable Department and FBI policies and guidelines, and a 2014 briefing paper prepared by FBI staff for Director Comey detailing the events surrounding the 2007 investigation and the applicable investigative standards currently in effect, including the new interim policy adopted by the FBI on June 8, 2016. We also interviewed FBI employees and a federal prosecutor who participated in the 2007 investigation and an FBI attorney who helped draft the 2014 briefing paper. In addition, we reviewed correspondence from the news media raising concerns regarding the undercover operation and the comments of Director Comey.

In Section III of this report, we identify the applicable Department and FBI policies and guidelines. In Section IV, we describe the facts and circumstances of the FBI's investigation of the 2007 Timberline bomb threats and the media's response to the FBI ruse to identify Jenkins. In Section V, we analyze whether the case agents followed the applicable guidelines in 2007 and whether different or additional approvals would be required under current Department and FBI policies.

III. Applicable Department and FBI Policies and Guidelines

A. Policies and Guidelines in Effect at Time of 2007 Investigation

1. Undercover Activity and Undercover Operations

In June 2007, the applicable FBI policies for online undercover criminal investigations were contained in the Manual of Investigative Operations & Guidelines, Part 2 (MIOG 2), Section 10-18; and the FBI's Field Guide for

[3] The FBI is in the process of incorporating the new interim policy into the Undercover Policy Guide, one of several policy implementation guides incorporated by reference into the FBI's Domestic Investigations and Operations Guide (DIOG). The DIOG sets forth FBI policies and procedures for all investigative activities and intelligence collection activities conducted by the FBI within the United States.

Undercover and Sensitive Operations (FGUSO). The MIOG 2 and the FGUSO incorporated the Attorney General's Guidelines on FBI Undercover Operations (AGG-UCO), and specifically with respect to online undercover investigations, also incorporated principles detailed in the Department's "Online Investigative Principles for Federal Law Enforcement Agents" (the Online Principles).[4] As we discuss later, both the MIOG 2 and the FGUSO were superseded by the FBI guidelines that are in effect today.

Section 10-18.5(a) of MIOG 2 permitted FBI employees to communicate online using false names or cover-identities and stated that undercover activity was governed by the FGUSO. While an FBI employee's use of another person's "online identity" in undercover online communications without that person's knowledge or consent required FBI Headquarters (FBIHQ) approval, FBI policy did not require special approval to use the identity of an organization or business in undercover online communications or in other undercover activities. MIOG § 10-8.5(4).[5] The FGUSO defined "undercover activities" as "any investigative activity involving the use of an assumed name or cover-identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI." Undercover activity in which an undercover employee planned to meet with a subject required the approval of a Supervisory Special Agent (SSA).

The FGUSO differentiated between "undercover activity" and an "undercover operation." It defined an "undercover operation" as "an investigation involving a series of related undercover activities over a period of time by an undercover employee." According to the FGUSO, this "generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation." Undercover operations had to be approved by the Special Agent-in-Charge (SAC) of the field office conducting the operation, in consultation with the Chief Division Counsel for the field office.

In regard to online undercover operations, the FGUSO specifically defined such operations as being "any investigation involving a series of related online covert contacts over a period of time by an Online Covert Employee (OCE)." According to the Online Principles, "[t]he nature of online communications makes counting undercover 'contacts' much more difficult than in the physical world. Generally, a physical-world contact consists of a single communication or conversation, either face-to-face or over the telephone, naturally circumscribed in time." The Principles state that "[c]ommunicating in cyberspace is different"

[4] The FGUSO was last updated on July 25, 2003. The current AGG-UCO was issued on May 30, 2002 and was modified on March 5, 2008, November 26, 2008, and November 22, 2015.

[5] Further, "untrue representations by a person participating in the undercover operation concerning the activities or involvement of any third person" without that person's knowledge or consent were considered "sensitive circumstances" under FBI policy and required FBIHQ approval. FGUSO § 3.2(F)(13). The undercover agent who communicated with Jenkins did not use the "online identity" of a person who was a member of the media, nor did he make untrue representations about any third person. Rather, the agent used the identity of a third party – the AP – without that party's knowledge or consent.

because the online conversation between the OCE and the subject is broken up by the send/receipt nature of online communications.

The FGUSO provided guidance to FBI agents about how to count online communications for purposes of undercover activities. The FGUSO stated that agents should count a discrete online "conversation" as one contact and identified numerous factors that agents should consider when deciding how to group distinct online transmissions into a single conversation. The FGUSO, quoting the AGG-UCO, stated that:

> In the context of online communications, such as e-mail and Internet Relay Chat (IRC), 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 in 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).

If based on these factors, an agent determined the undercover activity was expected to involve three or fewer "contacts," it was sufficient to obtain approval from the agent's supervisor. If the agent determined the activity was expected to involve more than three "contacts," the activity would constitute an "undercover operation" and required SAC approval. As discussed below, regardless of the number of contacts, if undercover activity or an undercover operation involved "sensitive circumstances," the field office was required to obtain FBIHQ approval.

2. Sensitive Circumstances

Under the FGUSO, undercover activity that involved "sensitive circumstances" constituted an undercover operation regardless of the number of contacts involved. Among the categories of "sensitive circumstances" identified in the FGUSO were "privileged relationships" in which:

> there [was] a reasonable expectation that the undercover operation [would] involve . . . [a] significant risk that a third party [would] enter into a professional or confidential relationship with a person participating in an undercover operation who [was] acting as an attorney, physician, clergyman, or *member of the news media*.

(Emphasis added) According to commentary included in the FGUSO regarding this provision, the professional or confidential relationships are listed in order to identify potential operational scenarios, including those in which "a relationship with a subject is established which the subject believes to be privileged." The commentary further states that while "[i]t 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 . . . their existence alone is a sensitive matter. . . ."[6]

The FGUSO required that in all undercover operations involving any sensitive circumstances, including online undercover operations, the SAC had to submit an application to FBIHQ seeking approval to begin the undercover operation. This application would then be reviewed by appropriate supervisory personnel at FBIHQ and, if favorably recommended, sent to the Criminal Undercover Operations Review Committee (CUORC) for consideration. The application would then be forwarded to the Director or a designated Assistant Director to approve or disapprove.

In regard to online undercover operations, Section 7.3 of the FGUSO permitted a SAC, or a designated Assistant Special Agent-in-Charge (ASAC), to grant interim authority for online undercover contacts involving sensitive circumstances. The interim authority, which must have been documented in writing, could be granted for up to 30 days and had to be followed by a report explaining the reason for granting the authority "as soon as practical."

3. Limitations on Online Undercover Activity

Section 10-18.3(1)(d) of MIOG 2 prohibited FBI agents from hacking into computers, including those belonging to subjects of FBI investigations, without legal authorization. Section 10-18.3 stated that "[s]oftware tools cannot be used to defeat the security system of [a] targeted electronic facility or access areas that are not already publicly viewable by general users of the system or the public absent a search warrant or other legal authorization." As an example, the provision identified Internet Protocol addresses as information that could not be obtained through software tools without legal authorization.

B. Applicable Policies and Guidelines Currently in Effect

In 2008, the FBI replaced the MIOG 2 with the Domestic Investigations and Operations Guide (DIOG). The DIOG was updated in October 2011.[7] In August

---

[6] Another category of "sensitive circumstances" under the FGUSO was "third party liability" and included:

> Untrue representations by a person participating in the [undercover operation] concerning the activities or involvement of any third person without that individual's knowledge or consent; [and]
>
> . . .
>
> Activities which create a realistic potential for significant claims against the United States arising in tort, contract, or for compensation for the "taking" of property, or a realistic potential for significant claims against individual government employees alleging Constitutional torts.

AGG-UCO, Section IV(C)(2)(o); FGUSO, Section 3.2(F). We did not find these provisions applicable to the undercover activities at issue in the Jenkins investigation: the undercover agent did not make untrue representations to Jenkins about any third person, and we do not believe the FBI's activities created a "realistic potential for significant claims against the United States" as contemplated by the FGUSO.

2011, the FBI replaced the FGUSO with the Undercover and Sensitive Operations Policy Implementation Guide (USOPIG). The DIOG and the USOPIG, like the FGUSO, incorporate the AGG-UCO. As such the USOPIG retained many of the provisions of the FGUSO, including the provisions relating to "sensitive circumstances," and is the FBI policy currently in effect regarding undercover activities and operations.[8] While these revised FBI policies included an additional provision that might have caused a field office to seek FBIHQ approval before an employee acted in an undercover capacity as a member of the media, the revised undercover policies did not require such a step.

On June 8, 2016, the FBI adopted an interim policy – referred to as Policy Notice (PN) 0907N, "Undercover Activities and Operations – Posing as a Member of the News Media or a Documentary Film Crew" – specifically governing situations in which FBI employees represent, pose, or claim to be members of the news media. The new policy sets forth the approval required to engage in such activity.[9] In essence it created an additional "sensitive circumstance" for undercover activity and is the operative policy currently in effect for purposes of our review.[10]

The new interim policy incorporates the DIOG's definitions of "undercover activity" and "undercover operation," which mirror the definitions contained in the FGUSO, as described earlier. In short, "undercover activity" is any investigative activity involving the use of an assumed identity by an undercover employee; an "undercover operation" is one that involves a "series of related undercover activities" – defined as five or more substantive contacts by an undercover employee with the individuals under investigation – over a period of time. However, under the new interim policy, the number of substantive contacts with an investigative subject is not a relevant factor in determining the level of approval required when posing as a member of the news media. This is because the policy expressly prohibits FBI employees from engaging in any undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized at FBIHQ as part of an undercover operation. DIOG § 8.1.3.1. and 11.9.1.

---

[7] All references to the DIOG in this section of the report are referring to the 2011 edition.

[8] The USOPIG and the DIOG include provisions that expressly address an FBI employee's use of another person's "online identity" in undercover online communications and the use of "untrue representations . . . concerning the activities or involvement of any third person" without that person's knowledge or consent. *See* DIOG 2, Appendix L; USOPIG § 3.2.6. However, similar to the FGUSO and the MIOG 2, neither the DIOG nor the USOPIG includes provisions that require special approval to use the identity of an organization or business in undercover online communications or in other undercover activities.

[9] The phrase "member of the news media" is defined as a person who "gathers, reports, or publishes news through the news media;" the phrase "news media" is defined as an entity that is "organized and operated for the purpose of gathering, reporting, or publishing news." DIOG § 10.1.2.2.5.

[10] As indicated by its title, the new interim policy applies to FBI employees posing as members of the news media or a documentary film crew. Our review addresses the policy only as it relates to employees posing as members of the news media.

Similar to undercover operations involving any of the "sensitive circumstances" delineated in the DIOG and USOPIG, the approval process for an undercover operation that involves an FBI employee posing as a member of the media requires the relevant FBI field office to submit an application to the Undercover Review Committee at FBIHQ for review. *Id.* § 8.2.2.1. In addition, the application can only be approved by the FBI Deputy Director, after consultation with the Deputy Attorney General. The FBI Deputy Director's approval cannot be delegated. *Id.*§ 8.2.2.1.3. The involvement of the Deputy Attorney General and the nondelegable nature of the FBI Deputy Director's authority are unique to applications for undercover operations involving FBI employees posing as members of the news media or a documentary film crew.[11]

C. Summary of Approval Requirements

The chart below summarizes the approval requirements for FBI undercover activities and operations, as well as the definition of "sensitive circumstances." Until recently, the approval requirements had remained essentially unchanged since 2007, when the Timberline bomb threat investigation was conducted. However, in November 2015, the Attorney General approved revisions to the AGG-UCO that included, among other changes, the requirement that a Department of Justice prosecutor and FBIHQ approve undercover activities that involve sensitive circumstances. None of those revisions impact this review. The more significant change for purposes of our review occurred in June 2016, when the FBI adopted interim policy, PN 0907N. This new policy prohibits FBI employees from posing as members of the news media, except as part of an undercover operation that is approved by the FBI Deputy Director after consultation with the Deputy Attorney General. The chart below reflects these changes in FBI policy.

[11] The new interim policy also includes procedures for authorizing undercover operations involving employees posing as members of the media under emergency circumstances, such as an immediate or grave threat to life or property, a threat to the national security, or the loss of a significant investigative opportunity. *See* DIOG §§ 8.2.4. to 8.2.4.2.

Type of Undercover Event	Current Review & Approval Requirements
Undercover Activity (not involving FBI employees posing as members of news media)	Supervisory Special Agent
Undercover Operation without sensitive circumstances[12]	Head of Field Office (Assistant Director in Charge or Special Agent in Charge)
Undercover Activity with Sensitive Circumstance(s)	Federal Prosecutor and FBIHQ
Undercover Operation with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ Approval
Undercover Operation involving FBI employees posing as members of the news media (not applicable in 2007)	Undercover Review Committee review and Deputy Director approval, after consultation with Deputy Attorney General

IV. OIG Factual Findings

A. The Timberline High School Investigation

On May 30, 2007 Timberline High School in Lacey, Washington was evacuated after a handwritten note containing a bomb threat was discovered at the school. On Sunday, June 3, 2007 an unknown subject, ultimately identified by the FBI as Timberline High School student Charles Jenkins, used a Gmail account to send an e-mail containing a bomb threat to numerous Timberline High School teachers and administrators. In the same e-mail, Jenkins threatened a "Distributed Denial of Service" (DDoS) attack on the school's computer network. The next day, school administrators evacuated the high school as a result of the threat and Jenkins launched his DDOS attack causing the school's networks to receive 24 million hits within a 24-hour period.[13]

[12] As noted above, in 2007, an undercover operation occurred when there were more than three substantive undercover communications. Under current policies, an undercover operation occurs where there are more than five substantive undercover communications.

[13] In a denial-of-service (DoS) attack, an individual attempts to prevent legitimate users from accessing information or services – such as on a website or in e-mail – by, for example, overloading the server that hosts the information or services with requests. In a DDoS attack, an individual uses multiple computers, sometimes thousands, to launch a DoS attack. *See* https://www.us-cert.gov/ncas/tips/ST04-015.

On June 5, 2007 Jenkins sent another e-mail containing a bomb threat from a different Gmail account to the high school principal and other high school staff. School administrators again evacuated Timberline High School as a result of this threat. That same day, and using a third Gmail account, Jenkins sent a fourth bomb threat to Timberline High School staff in which he taunted school officials, stating:

> Maybe you should hire Bill Gates to tell you that [this e-mail] is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be "tracing it" because I have already told you it's coming from Italy. That is where any trace will stop so just stop trying. Oh and this email will be behind a proxy behind the Italy server.[14]

The Lacey Police Department investigated the bomb threats by interviewing persons of interest and identifying the Internet Protocol (IP) addresses that were the source of the e-mails.[15] Investigators were able to establish that Jenkins was using two IP addresses based in Italy and one based in the Czech Republic. The investigators believed that these IP addresses were proxies and did not indicate Jenkins's true location.

On June 6, 2007 Jenkins used a fourth Gmail account to send an e-mail to Timberline High School's principal stating, "ENJOY YOUR LIFE ENDING." In another e-mail, from the same Gmail account, Jenkins sent a bomb threat to Timberline High School teachers in which he again taunted authorities' efforts to identify him. School administrators evacuated Timberline High School as a result of this threat.

That same day, officers from the Lacey Police Department contacted the Northwest Cybercrime Task Force (NWCTF), which was supervised by SSA Lucas Johnson of the FBI's Seattle Division, and requested assistance in identifying and apprehending Jenkins.[16] The FBI opened its investigation immediately and confirmed that the IP addresses being used to send the bomb threats were based in Grumello Del Monte, Italy and the Czech Republic. The FBI agents also contacted Assistant U.S. Attorney (AUSA) Chloe Watson for assistance, which she provided by working with agents to prepare the court documents in the case, as discussed below.[17]

Also on June 6, 2007 Detective Tyler Dawson of the NWCTF sent an e-mail to the FBI's Legal Attaché in Rome, Italy, requesting his assistance in working with the

---

[14] A "proxy" is a server that functions as a relay between the user and a destination website. A proxy hides the IP address of the user's machine from the website.

[15] An "IP Address" is a code made up of a unique set of numbers that identifies a computer on the Internet.

[16] Lucas Johnson is a pseudonym.

[17] Chloe Watson is a pseudonym.

Italian government to identify Jenkins.[18] In his request, Dawson included all of the potentially identifying information contained in the bomb threats made by Jenkins, including known IP addresses.

The next day, June 7, 2007, Jenkins sent another bomb threat from the e-mail address thisisfromitaly@gmail.com. School administrators again evacuated Timberline High School. Jenkins also posted three threatening messages in the comments section of the "theolympian," the online version of a Washington state newspaper, *The Olympian*.

That same day, Jenkins created a profile on the social networking site, Myspace.com, entitled "Timberlinebombinfo" and invited 33 Timberline High School students to post a link to the Myspace page. Jenkins also threatened at least one student by telling her that if she failed to post the link, her name would be associated with future bomb threats. Two of the students who received the request to link to Jenkins's Myspace.com page reported the request to local police.

On June 7, 2007 law enforcement officials from the Lacey Police Department met with Johnson, FBI Special Agent Mason Grant, Detective Dawson, other FBI officials, and Watson.[19] During the meeting, the FBI agents agreed that they would seek a court order authorizing the use of a trap and trace device for the phone of a suspect, and request the FBI's Behavioral Analysis Unit to develop a behavioral assessment of Jenkins.[20] The agents also agreed to pursue court authorization to utilize a Computer & Internet Protocol Address Verifier (CIPAV) that would allow the FBI to "identify the computer and/or user of the computer that [were] involved in" making the bomb threats against Timberline High School. According to FBI documents, "[t]he deployment of the CIPAV would require an undercover scenario to entice [Jenkins] to download the code concealing the CIPAV." The same day as the meeting of law enforcement officials, Grant began drafting the affidavit in support of a warrant seeking authority to surreptitiously install a CIPAV.

On June 8, 2007 the school district received two additional bomb threats that resulted in the evacuation of Timberline High School. That same day, Johnson contacted SSA Keith Pratt, a certified behavioral analyst with an FBI Behavioral Analysis Unit, to obtain Pratt's help developing a behavioral assessment of Jenkins.[21]

On June 10, 2007 Grant submitted a "Notification of SAC/ASAC Authority Granted for Use of Telephonic and/or Nontelephonic Consensual Monitoring Equipment in Criminal Matters" (the Notification) to ASAC Mike Higgins seeking

---

[18] Tyler Dawson is a pseudonym.

[19] Mason Grant is a pseudonym.

[20] On June 8, 2014, Watson filed under seal the application to use the pen register device. The U.S. District Court for the Western District of Washington approved the application that same day. The FBI determined that the suspect for whom they obtained the pen register was not the individual e-mailing the bomb threats.

[21] Keith Pratt is a pseudonym.

approval to use the CIPAV.[22] Among other things, the Notification required Grant to provide a synopsis of the case and to identity the individual whose communications would be consensually monitored. The Notification form listed six specific situations that required written DOJ approval prior to proceeding with the consensual monitoring, none of which applied to the bomb threat investigation.[23] The Notification did not describe how the agents intended to deploy the CIPAV. Although not required, the request did not include any mention that agents intended to pose as a journalist in order to facilitate the successful use of the CIPAV. Higgins approved Grant's request to use the CIPAV the same day it was submitted.

The Seattle Division requested a CIPAV from the FBI's Operational Technology Division/Cryptologic and Electronic Analysis Unit (OTD/CEAU) on June 11. The agents from OTD/CEAU were responsible for creating the CIPAV that would be used to locate Jenkins. Johnson and Grant also spoke with Pratt, the certified behavioral analyst who conducted the behavioral assessment of Jenkins. Pratt told us that Jenkins appeared to be very narcissistic and was feeding off of the attention he was receiving as a result of the bomb threats. Pratt stated that he recommended that the agents use that narcissism to override any suspicions that Jenkins might have about clicking on the link that would deploy the CIPAV, and suggested the link could have "some type of story or media report about him." Watson told us that she did not recall participating in a conference call with Pratt, but that Grant might have told her about the consultation with the Behavioral Analysis Unit and about Pratt's recommendation that the FBI use a media approach to deploy the CIPAV.

---

[22] Mike Higgins is a pseudonym.

[23] The six situations identified on the form as requiring Department approval were the following:

> 1. Monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous 2 years;
>
> 2. Monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any State or Territory, & the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his/her official duties;
>
> 3. Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country;
>
> 4. Consenting/nonconsenting party is or has been a member of the Witness Security Program & that fact is known to the agency involved or its officers;
>
> 5. Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service; and
>
> 6. Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

Johnson told us that his investigative team had spent some time discussing the possible scenario proposed by Pratt. He stated that he believed that posing as a reporter could be problematic because a reporter's name could be easily verified. For this reason, the team decided to use a publisher or editor's name because it would not be readily identifiable by Jenkins. On the subject of whether the scenario would qualify as a "sensitive circumstance," Grant told us that he could not recall anyone considering that. However, Johnson told us that he consulted the FGUSO to assess this issue and concluded that the scenario was not a sensitive circumstance. Johnson said that even though the undercover employee would pose as a member of the news media, the contact would be limited to building the credibility necessary to convince Jenkins to click on the link and activate the CIPAV. Johnson also said they had no intention to publish anything or contact a third party.

Johnson told us that while he was not aware of a legally-recognized "reporter-source" privilege, he believed that a person acting as a source of information for a reporter could enter into a privileged relationship with that reporter. Asked whether he had any concerns that Jenkins would enter into or believe he was entering into a privileged relationship with the undercover agent, Johnson told us that he did not. Johnson also said it was his responsibility to research the applicable FBI policies and make the "judgment call" that the proposed undercover contact was not a sensitive circumstance.

AUSA Watson told us that she did not recall anyone telling her about a plan to impersonate a member of the news media to deploy the CIPAV. She told us that she was not involved in the operational aspect of the undercover activities and that the agents did not need her approval for how they would deploy the CIPAV. Consistent with Watson's recollection, we found no FBI documents which reflect or suggest knowledge or approval by Watson of the ruse to impersonate a journalist. Based on our investigation, we found no evidence that any other attorney at the U.S. Attorney's Office or the FBI was asked to consider whether such a tactic was appropriate.

Also on June 11, 2007 SSA Johnson briefed ASAC Higgins "on the facts of the investigation and the need to engage in limited on-line [undercover] communication with [Jenkins] for the purpose of deploying the CIPAV." According to an FBI document describing the briefing, the investigative team did not anticipate more than three substantive contacts with Jenkins and there was no expectation that there would be a face-to-face meeting between an undercover agent and Jenkins. The document did not reflect the plan to pose as a member of the media, but Johnson told us that he discussed at the briefing the fact that the undercover agent would attempt to get Jenkins to click on a link that would deploy the CIPAV by posing as a member of the media. Johnson also said that he believes he would have given Higgins his opinion, based on his review of FBI policy, that the undercover activities did not involve sensitive circumstances.

Higgins told us that it was common for Johnson to brief him on matters for cases that required approval above Johnson's level, especially for matters involving electronic eavesdropping requests, which required approval before applications

could be submitted to the court. However, Higgins told us that he had no "independent recollection" of the Timberline High School bomb threat investigation.

On June 12, 2007 the investigative team drafted a fake news article with an Associated Press (AP) byline entitled "Bomb threat at high school downplayed by local police department." Grant attached the fake news article to a draft e-mail that he proposed to send to Jenkins. The proposed e-mail contained a hyperlink to the fake news article that read: "http://seattletimes.nwsource.com/html/nationworld/2003743231_webteensex11.html" and included advertisements relating to *The Seattle Times*. He forwarded the proposed e-mail and fake news article to the special agents in OTD/CEAU who were creating the CIPAV, and to Johnson. The assigned OTD/CEAU agent responded to Grant that he would be able to use the fake article to deploy the CIPAV into Jenkins's computer.

That same day, AUSA Watson filed an application with the U.S. District Court for the Western District of Washington in Seattle that requested permission for the FBI to use the CIPAV to target "any computer accessing electronic message(s) directed to administrator(s) of myspace account 'timberlinebombinfo' and opening message(s) delivered to that account by the government, without notice to the owner/operator of that computer." Watson filed an affidavit with the application that was written and affirmed by Grant. The affidavit did not provide specific details about the contents of the FBI's message that would be sent to the unknown subject or advise the judge that agents intended to impersonate a journalist as part of their ruse.

Watson told us that while she did not write the affidavit, it was her practice to review first drafts of affidavits and communicate with agents regarding any questions relating to probable cause. In the affidavit, Grant described the facts and circumstances of the investigation and explained how the CIPAV worked. The affidavit stated that a communication containing the CIPAV would be delivered to the unknown subject's computer "through an electronic messaging program from an account controlled by the FBI" that would be "directed to the administrator(s) of the 'Timberlinebombinfo' account." The affidavit also stated that "[o]nce the CIPAV is successfully deployed, [the CIPAV] will conduct a one-time search of the activating computer and capture" the computer's IP address and other information, which would then be sent to a computer controlled by the FBI.[24] The Court approved the government's application the same day it was filed.[25]

Grant told us that he did not include in the affidavit the information about how the FBI intended to deliver the CIPAV, including the fact that they intended to

[24] At no time did the FBI file a Title III wiretap application as some news organizations had reported.

[25] The application and Sander's supporting affidavit were reviewed by AUSA Watson and an attorney from the Office of General Counsel for OTD prior to being filed with the Court. Although there was no requirement that they do so, neither document mentioned the existence of the FBI's plan to impersonate a journalist.

pose as a member of the media, because it was not needed to secure the court order. He stated further that law enforcement agencies typically do not want to expose details of undercover techniques in case they need to use the techniques in future investigations. Watson told us that information regarding how the FBI would execute a search warrant was not typically included in the affidavit supporting the search warrant because information was not needed to obtain the Court's approval. She also said that she could not recall any search warrant she had ever worked on that described how the warrant "would be affected."

That evening, at 5:38 p.m., Grant used an undercover e-mail account to send an e-mail containing a link to the fake news article containing the CIPAV to the Myspace page, "Timberlinebombinfo." Jenkins did not respond to this e-mail. The next day, at 2:51 p.m. on June 13, 2007, Grant used the same undercover e-mail account to send a second e-mail with the link to the fake news article containing the CIPAV to "timberlinebombinfo."[26] Grant's e-mail stated:

> Disappointed that I did not get a response from my "anonymous" interview request. The article was not published in today's papers, but my Staff Writer drafted an updated version and we left blanks if you would like to comment. . . .

Grant identified himself in the e-mail as "Norm Weatherill," an "AP Staff Publisher."

At 2:55 p.m. Jenkins responded, "leave me alone." Grant replied at 3:21 p.m.:

> 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. . . .

According to Grant, this message was intended to get Jenkins to click the link to the fake news story. He said the entire investigative team was present during this and the other communications with Jenkins, and consulted together about what to say before the message was sent. According to Johnson, the 3:21 p.m. reply to Jenkins drew upon the recommendation of the Behavioral Analysis Unit to play on Jenkins's ego and to build rapport. Johnson said the investigative team was trying to take

[26] The agents identified the link to the unknown subject as "news article." The hyperlink, which was not visible Glazebrook, was: "http://reporting.homeip.net:81/private/596169732/articlestuff.exe."

advantage of the desire for attention Jenkins demonstrated with his online activity, while also assuring Jenkins that he was only being asked for his side of the story, and not to disclose his identity.

Jenkins responded to Grant's message 2 minutes later by inquiring, "how can i (sic) help." Grant responded by asking Jenkins if the article and pictures were accurate. At approximately 3:30 p.m., Jenkins clicked on the link to the fake news article with the embedded CIPAV. However, because of certain settings on Jenkins's computer, the CIPAV did not deploy. At 3:47 p.m. Jenkins e-mailed Grant and asked him to engage in a live chat on Gmail. The two began their conversation at 3:48 p.m. Among other things, Jenkins asked Grant what organization he was with. Grant responded that he was with the "Associated Press," and added that "AP [articles] can be found in [the] NY Times, Seattle Times, Washington Post, US[A] Today or even local papers – such as the Olympian."

At 5:07 p.m., Jenkins contacted Grant through live chat on Gmail asking if he had "any news yet." At 5:50 p.m., Grant responded via e-mail that "they are crunching the article now," and sent him the link to some photographs related to the article that were embedded with a CIPAV. Jenkins clicked on the link to the photographs and e-mailed Grant at 5:53 p.m. stating, "dont (sic) care about which pics you use." This time, when Jenkins clicked on the link to the photographs, the CIPAV deployed properly and the FBI obtained his true IP address.

Using the true IP address, the FBI was able to locate and then identify Jenkins, a 10th grade student at Timberline High School, as the individual who had been e-mailing the bomb threats to the school. At approximately 2:00 a.m. on June 14, 2007, the Lacey Police Department executed an arrest warrant on Jenkins and arrested him at his parents' house. Upon arrest, Jenkins immediately confessed to sending multiple bomb threats to the Timberline School District. Two additional draft bomb threats were found on his computer at the time of his arrest.

That same day, Johnson drafted and submitted an "FBI Urgent Report" addressed to then-FBI Director Robert Mueller and other FBI divisions. The report, entitled "Other Matter Warranting the Immediate Attention of FBIHQ Executives," included a synopsis of the FBI's investigation of Jenkins and specifically stated that the "CIPAV was deployed through an undercover electronic message session between Seattle undercover employees and Jenkins." The report did not describe the tactic of impersonating a journalist.

The State of Washington prosecuted Jenkins after the U.S. Attorney's Office declined prosecution because Jenkins was a juvenile. On July 16, 2007 Jenkins pleaded guilty to three counts of identity theft (Class C Felony), two counts of Threat to Bomb or Injure Property (Class B Felony), and one count of Felony Harassment (Class B Felony). He was sentenced that same day to 90 days of juvenile detention, 2 years of supervised release, 2 years of mental health counseling, and 2 years of probation with restrictions on internet and computer usage. Jenkins was also expelled from the Timberline School District.

B. Media Response to the FBI's Investigation of Jenkins

The FBI did not publicize the assistance its agents provided to the Lacey Police Department during the investigation of Jenkins's bomb threats. However, on July 18, 2007, 2 days after Jenkins pleaded guilty, the online technology news website, Wired.Com, released an article entitled "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats." The article explained how the CIPAV worked and how the FBI used it to locate Jenkins. The article did not reference the fact that the FBI had impersonated a member of the news media.

Seven years later, on October 27, 2014, *The Seattle Times* released an article based upon e-mails obtained by the Electronic Frontier Foundation (EFF) through a Freedom of Information Act request. The e-mails obtained by the EFF disclosed the fact that the FBI posed as a member of the press when it contacted and then identified Jenkins as the author of the bomb threats.

On October 30, 2014, the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's use of a fake AP news story in connection with its investigation of the bomb threats. In its letter, the AP's General Counsel, Karen Kaiser, complained that the AP learned, "more than seven years after the incident occurred," that "the FBI both misappropriated the trusted name of the Associated Press and created a situation where our credibility could have been undermined on a large scale." Kaiser added, "It is improper and inconsistent with a free press for government personnel to masquerade as The Associated Press or any other news organization." She said the FBI's actions "undermined the most fundamental component of a free press – its independence." In addition, several newspapers wrote articles questioning the tactics the FBI used to identify and arrest Jenkins.

In response to these news articles in 2014, FBI employees in the Cyber Division worked with attorneys in the FBI's Office of General Counsel (OGC), Cyber Law Unit, to draft a "Situation Action Background" (SAB) report that described the facts and circumstances surrounding the FBI's investigation and identification of Jenkins. The OGC attorney primarily responsible for drafting the SAB told us that the document was created to inform FBI executive leadership about the FBI's actions to identify and apprehend Jenkins. The SAB also included OGC's analysis of the applicable Department and FBI policies in effect at the time of the investigation, as well as OGC's analysis of the applicable Department and FBI policies currently in effect.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's investigation. Consistent with OGC's analysis in the SAB, Comey stated that the "technique [the FBI used to identify and apprehend Jenkins] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

The same day, the Reporters Committee for Freedom of the Press (RCFP), on behalf of 25 other news organizations, wrote a letter to Holder and Comey voicing

its objection to the FBI impersonating journalists. In the letter, the RCFP complained, "[t]he utilization of news media as a cover for delivery of electronic surveillance software is unacceptable. This practice endangers the media's credibility and creates the appearance that it is not independent of the government. It undermines media organizations' ability to independently report on law enforcement. It lends itself to the appearance that media organizations are compelled to speak on behalf of the government." The RCFP urged "the Attorney General and FBI to clarify that impersonation of the media is unacceptable. . . ." The letter further asserted that the operation "should have been subjected to heightened review and scrutiny, disclosed to OGC and the magistrate judge, and evaluated for what it was – an investigation that involved significant First Amendment concerns."

V. OIG Analysis, Conclusions, and Recommendation

In this section, we assess whether, under Department and FBI policies in effect at the time of the 2007 investigation, appropriate approval was obtained for the undercover activities the FBI conducted to locate Jenkins. We concluded that Department and FBI policies in effect in 2007 did not prohibit agents from impersonating journalists or from posing as a member of a news organization, nor was there any requirement that agents seek special approval to engage in such practice. The only policies in effect at the time that might have required elevated consideration regarding the FBI's plans turned on whether the undercover activity involved a "sensitive circumstance." We concluded, given the lack of clarity in the policy language, that making a determination about the required approvals was a challenging one and that the judgments made by the agents were not unreasonable. However, we also concluded that after the plan was launched and Jenkins indicated to the undercover agent that he wanted to be left alone, the investigative team should have considered whether a message to Jenkins that included an implied offer of confidentiality would create a "sensitive circumstance" requiring a higher level of approval before the message was sent.

We also assess in this section whether those same undercover activities conducted in 2007 would require a higher level of approval under Department and FBI policies currently in effect. We concluded that an interim policy change adopted by the FBI on June 8, 2016 would prohibit the 2007 undercover activities unless they were part of an undercover operation reviewed by the Undercover Review Committee at FBIHQ and authorized by the FBI Deputy Director, after consultation with the Deputy Attorney General.

A. Policies in effect in 2007

In 2007, FBI policies did not prohibit the practice of agents impersonating journalists, nor was there any requirement that agents seek special approval to engage in such practice. Instead, agents were left to consult with the more general undercover policies which implicitly prohibited impersonation of a member of the news media only if there was a "significant risk" that a third party would enter into a confidential relationship with the undercover FBI employee.

There essentially were three questions that had to be answered in 2007 regarding the proposed online undercover activity to determine what level of approval was required before the activity was initiated. First, was the proposed activity in fact "undercover activity"? Second, how many "substantive undercover contacts" were expected to occur between the undercover employee and the subject of the investigation? Third, did the undercover activity involve any "sensitive circumstances"? As summarized in the following table, the answers to these questions established the level of approval required:

Type of Undercover Event	**Review and Approval Requirements**
Undercover Activity with 3 or fewer contacts	Supervisory Special Agent
Undercover Operation (*i.e.*, undercover activity more than 3 contacts)	Head of Field Office
Undercover Activity with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ Approval
Undercover Operation with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ approval

The FBI's plan to locate Jenkins clearly was undercover activity, that is, "any investigative activity involving the use of an assumed name or cover-identity by an employee of the FBI . . . ." The plan called for an agent to pose as an editor working for the AP and contact Jenkins by e-mail for purpose of surreptitiously installing a computer program – the CIPAV – that would reveal the location of the computer Jenkins was using. This plan constituted "undercover activity" under FBI policy.

The agents involved in the development of the plan anticipated that it would require three or fewer substantive contacts with Jenkins to install the CIPAV. We do not believe this was an unreasonable expectation. The bomb threats alone were brazen, and in the e-mails communicating the threats, Jenkins was arrogant and dismissive of the authorities' efforts to locate and identify him. Further, Jenkins created a public profile on Myspace.com and invited 33 of his classmates to post links to the page, even threatening one student that if she failed to do so, he would associate her with the next bomb threat. We believe that in view of Jenkins's display of conceit and his contempt for the efforts to locate him, it was not unreasonable to expect that he would respond quickly to an inquiry from the media about the bomb threats, and that it would therefore probably not take more than three online "contacts" to deploy the CIPAV.

We believe that the third question that had to be addressed – whether the undercover activity involved a "sensitive circumstance" – was a difficult one.

However, we ultimately concluded that SSA Johnson's judgment that the plan did not involve a sensitive circumstance was not unreasonable.

As described in this report, the plan to get the CIPAV installed on Jenkins's computer would implicate the category of sensitive circumstances referenced in the FGUSO involving "privileged relationships" if there was:

> a reasonable expectation that the undercover operation would involve . . . [a] significant risk that a third party [would] enter into a professional or confidential relationship with a person participating in an undercover operation who [was] acting as . . . [a] member of the news media.

According to FBI policy guidance, this sensitive circumstance extended to scenarios where a relationship with a subject was established that the subject believed was privileged. The plan in the Jenkins investigation was for the undercover agent to represent himself to Jenkins as a journalist working for the AP in order to entice Jenkins to click on a link to a fake news article. The idea to use a "press angle" originated with the FBI analyst who conducted a behavioral assessment of Jenkins. The analyst told the agents and the AUSA that this approach would "play on [Jenkins's] ego." Also, SSA Johnson told us that he consulted the relevant policy manual and concluded that the plan did not present a sensitive circumstance because, even though the undercover agent would pose as a member of the media, the communication would be limited to establishing the credibility needed to get Jenkins to click the link to the fake news article. There was no intention or expectation that they would be engaging in protracted discussions with Jenkins, or any need or attempt to enter into a confidential or privileged relationship with him.

According to witnesses, the press angle they decided to use in the contact with Jenkins was intended to take advantage of his ego and to establish the undercover agent's credibility. The plan did not entail an attempt to develop a confidential relationship with Jenkins. Considering this, and the agents' belief that it would take three or fewer contacts with Jenkins to get the CIPAV deployed, we found that it was not unreasonable for SSA Johnson to conclude at the outset of the undercover activity that there was not a "significant risk" that Jenkins would enter into a confidential relationship with a member of the media, and that therefore the undercover activity did not include a sensitive circumstance.

Having concluded that the judgments the agents made about the anticipated number of online contacts between the FBI and Jenkins and whether any "sensitive circumstances" existed were not unreasonable, we found – as indicated in the table above – that it was permissible for SSA Johnson to approve the online undercover activity.

However, the FBI knew little about Jenkins and could not predict with any reasonable degree of confidence how he would react to the undercover contact. Indeed, Jenkins did not respond to the agent's first communication, and when he did reply to the second, it was to tell the agent to "leave me alone." It was only after the agent told Jenkins that he was not trying to determine his true identity, and that he "would rather not know who you are as writers are not allowed to

reveal their sources," that Jenkins expressed a willingness to help.[27] We highlight this – that is, how the plan actually unfolded – not because it proves the agents' advance assessment of the plan was wrong, but to demonstrate the plan's inherent unpredictability and of the potential need to reassess the necessary approval requirements.

We considered whether the level of approval required for the undercover activity changed after the plan was launched based upon either the number of substantive contacts the undercover agent was having with Jenkins or the content of the communications. With respect to the number of substantive contacts, and considering the guidance the FBI provided agents for counting online contacts, we did not find a basis to question whether the level of approval required should have been reevaluated as the plan unfolded. However, with respect to the content of the communications, we found that the message to Jenkins assuring him that his identity would not be revealed had the potential to cause Jenkins to believe he was entering into a confidential relationship with the undercover agent. At this point, we believe the investigative team should have re-evaluated the situation and consulted with their SAC before sending the additional message.

As noted above and described in Section III, Jenkins did not respond to the undercover agent's first e-mail message, and in response to the agent's second message replied, "leave me alone." At that point, the investigative team discussed what to say in response. The message that was sent to Jenkins included assurances that they were not trying to identify him – "[a]s a member of the Press, I would rather not know who you are as writers are not allowed to reveal their sources." According to SSA Johnson, the message was intended to play on Jenkins's ego and build rapport, and to take advantage of his desire for attention while assuring him that he was not being asked to disclose his identity. As described earlier, Jenkins responded to this message 2 minutes after it was sent with his offer to help.

We believe the assurance made to Jenkins – particularly the statement that "writers are not allowed to reveal their sources" – was an implied promise of confidentiality. As such, it created a risk that Jenkins would believe he was entering into a confidential relationship with an undercover agent acting as a member of the news media. The investigative team did not adequately consider whether that risk was "significant" and therefore whether a "sensitive circumstance" existed under the FGUSO's "privileged relationships" provision. Had the team concluded that the message prepared for Jenkins created a significant risk, FBI policy accommodated operational needs by authorizing the SAC, or designated ASAC, to grant interim authority for online undercover contacts involving a sensitive circumstance. Thus, although FBIHQ and CUORC ultimately would have had to

[27] This implicit promise of confidentiality, made by an undercover agent posing as a journalist, was one of the objections the media raised about this practice out of a concern that it could make potential sources leery of trusting journalists for fear they might actually be police or agents posing as journalists.

approve the activity, there was a mechanism by which the investigative team could have continued its engagement with Jenkins with little delay.

After reviewing a draft of this report, the FBI told us that it concurred with our conclusion that the "privileged relationships" provision applies to scenarios involving subjects of investigations as well as third parties. However, the FBI provided the OIG with comments that indicated to us that the scope and application of the FGUSO's "privileged relationships" provision is potentially susceptible to multiple interpretations. This was also evident in interviews we conducted during the course of this review. In light of the fact the current FBI policy – the USOPIG – fully incorporates the FGUSO provision, including the associated commentary, we believe it is important that the FBI provide clear guidance to employees about the circumstances to which the provision is meant to apply. Therefore, we recommend the FBI consider whether revisions to the USOPIG are required to ensure that undercover activity involving a significant risk that a subject believes he has entered into a privileged relationship with an undercover agent, is treated as a "sensitive circumstance."[28]

B. Policies in effect today

We also assessed whether those same undercover activities conducted in 2007 would require a higher level of approval if conducted under Department and FBI polices currently in effect today. As described in Section III.B. of this report, on June 8, 2016, the FBI adopted an interim policy – PN 0907N – that prohibits FBI employees from engaging in undercover activities that involve posing as members of the news media, unless those activities are authorized as part of an undercover operation by the Deputy Director, after consultation with the Deputy Attorney General. The number of substantive contacts by an undercover employee with the individual under investigation is no longer a relevant factor under this policy as it applies to employees posing as members of the news media.

The AP is "organized and operated for the purpose of gathering, reporting, or publishing news" and clearly falls within the definition of "news media" under FBI policy. It is equally clear under FBI policy currently in effect, that any undercover activity that would involve an employee posing as a member of the AP would have to be approved as an undercover operation at FBIHQ. The head of the FBI field office proposing the activity would first have to approve the application for the undercover operation to be submitted for approval to FBIHQ; the Undercover Review Committee at FBIHQ would then be required to review the application; and the Deputy Director, after consulting with the Deputy Attorney General, would be responsible for approving the application.

[28] As discussed earlier, the FBI's June 2016 interim policy applies to employees posing as members of the news media or as a documentary film crew. The types of privileged relationships covered by the USOPIG include those with an attorney, physician, or clergyman, as well as with a member of the news media. Therefore, the June 2016 interim policy does not obviate the need to provide clear guidance on the scope and application of the discussed USOPIG provision.

We believe the June 2016 policy on FBI employees posing as members of the news media is a significant and important improvement to FBI policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June 8, 2016. The Department and the FBI have previously implemented a number of policies addressing the use of law enforcement tools to obtain information from or about members of the news media in criminal and civil investigations. Since 1980, federal regulations have required the Attorney General to authorize subpoenas issued to or for the telephone records of any member of the news media. *See* 28 C.F.R. § 50.10(e). Those regulations, which also governed the interrogation, indictment, or arrest of members of the news media, were re-examined by the Attorney General in 2013 at the direction of the President. The re-examination followed public criticism of the Department's actions in issuing subpoenas for 2 months of records related to 20 telephone lines used by AP staff as part of a criminal investigation into the unauthorized disclosure of classified information.[29]* Following the Attorney General's review, the Department amended these regulations in February 2014 in order to "provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering activities," *see* 28 C.F.R. § 50.10(a), and to "ensure more robust oversight by senior Department officials; centralize the internal review and evaluation process; [and] set out specific standards for the use and handling of information obtained from, or records of, members of the news media . . . ." Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media, 79 F.R. § 10989-01 (2014).

While impersonating a member of the media potentially implicates different First Amendment concerns than using tools such as subpoenas and court orders to obtain information directly from news organizations, the activity also has the potential to "impair newsgathering activities" by, for example, making it less likely that sources will share information with journalists, fearing they might actually be FBI agents posing as journalists. The FBI's June 2016 interim policy on undercover activities that involve agents posing as members of the news media is an important and appropriate addition to the policies the Department previously implemented to regulate certain law enforcement activities that affect members of the news media.

Finally, as we described in Section III of this report, we learned during the course of this review that while FBIHQ approval is required to use a third person's "online identity" in undercover online communications or to make "untrue representations . . . concerning the activities or involvement of any third person" without that person's knowledge or consent, special approval was not required to use the identity of an organization or business in undercover online communications

---

[29] *See, e.g.*, https://www.washingtonpost.com/world/national-security/under-sweeping-subpoenas-justice-department-obtained-ap-phone-records-in-leak-investigation/2013/05/13/11d1bb82-bc11-11e2-89c9-3be8095fe767_story.html (accessed August 3, 2016).

* An earlier version of this report incorrectly stated that the subpoenas were issued to the AP.

or in other undercover activities. The new interim policy changes that policy as it relates to news organizations, but does not address this issue with regard to non-news organizations or businesses. We think the Department should consider the appropriate level of review necessary before agents in a criminal investigation are allowed to use the name of a third-party organization or business without its knowledge or consent, in light of the potential impact that use might have on the third party's reputation.[30]

C. Conclusion and Recommendations

We found that Department and FBI policies in effect in 2007 did not prohibit agents from impersonating journalists or from posing as a member of a news organization, nor was there any requirement that agents seek special approval to engage in such undercover activities. The only policies in effect at the time that might have required elevated consideration regarding the FBI's plans turned on whether the undercover activity involved a "sensitive circumstance." We concluded, given the lack of clarity in the policy language, that making a determination whether a situation was a "sensitive circumstance" was a challenging one and that the judgments made by the agents were not unreasonable given the lack of clarity. However, we also concluded that after the plan was launched, the investigative team should have considered whether a message to Jenkins that included an implied offer of confidentiality would create a "sensitive circumstance" requiring a higher level of approval before the message was sent.

We also found that prior to the adoption of the new interim policy in June 2016, FBI policy would not have prohibited FBI employees from engaging in the undercover activities agents conducted during the 2007 Timberline investigation. The new interim policy, however, clearly prohibits FBI employees from engaging in an undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized as part of an undercover operation. In order for such an operation to be authorized, the undercover application must first be approved by the head of the FBI field office submitting the application to FBIHQ, reviewed by the Undercover Review Committee at FBIHQ, and approved by the Deputy Director, after consultation with the Deputy Attorney General.

We believe the new interim policy on undercover activities that involve FBI employees posing as members of the news media is a significant improvement to FBI policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June

[30] After reviewing a draft of this report, the FBI provided comments explaining that the heightened level of review and approval required for FBI employees to pose as members of the news media was introduced because such activity potentially could "impair newsgathering activities" under the First Amendment, but that such constitutional considerations do not apply to businesses and other third parties. Our recommendation, however, does not rely on equating the reputational interests of some third party organizations and businesses with the constitutional interests of others. We believe that reputational interests, and the potential impact FBI investigations can have on those interests, are themselves sufficiently important to merit some level of review before FBI employees use the names of third party organizations or businesses without their knowledge or consent.

2016. The new interim policy also is an important extension of policies the Department has previously implemented to regulate certain law enforcement activities that affect members of the news media, such as obtaining information from or about members of the news media in criminal and civil investigations. The FBI should move expeditiously to update its undercover policy guide to incorporate this new interim policy, and widely inform and educate FBI employees about the policy's existence and application.

Based upon our review, we make three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurs with the recommendations.

Recommendation 1: The FBI should move expeditiously to update its undercover policy guide to incorporate the June 2016 interim policy on undercover activities in which FBI employees represent, pose, or claim to be members of the news media or a documentary film crew; and widely inform and educate FBI employees about the policy's existence and application.

Recommendation 2: The FBI should consider the appropriate level of review required before FBI employees in a criminal investigation use the name of third-party organizations or businesses without their knowledge or consent.

Recommendation 3: The FBI should consider whether revisions to the USOPIG are required to ensure that undercover activity involving a significant risk that a subject believes he has entered into a privileged relationship with an undercover agent, is treated as a "sensitive circumstance."

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig