UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ASSOCIATED PRESS, *et al.*, Plaintiffs, v. FEDERAL BUREAU OF INVESTIGATION, Defendant.	)	Civil Action No. 16-cv-1850 (TSC)

MEMORANDUM OPINION

Before the court are cross motions for summary judgment in this case brought under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. In 2016, Plaintiffs Associated Press, Gannett Satellite Information Network d/b/a USA Today, and Vice Media, LLC ("Plaintiffs"), each filed FOIA requests to the Federal Bureau of Investigation ("FBI") for records relating to an agreement with a technology vendor who assisted the FBI in unlocking the iPhone of a suspected terrorist. As part of the parties' joint agreement in this litigation, the FBI has produced 100 of 123 responsive pages in full or in part, with certain material withheld pursuant to FOIA Exemptions 1, 3, 4, 6, 7(C), and 7(E). Plaintiffs have narrowed their FOIA request on summary judgment to two specific pieces of information—the identity of the vendor, and the price paid to the vendor—such that only Exemptions 1, 3, 4, and 7(E) remain disputed. The FBI claims that Exemptions 1, 3, and 7(E) apply independently to the identity of the vendor and the purchase price, and that Exemption 4 also applies independently to the purchase price.

Plaintiffs have also moved to supplement the record with then-FBI Director James Comey's May 3, 2017, Senate testimony. The court will GRANT Plaintiffs' motion to supplement the record and consider the testimony as part of Plaintiffs' brief.

Upon consideration of the parties' filings, the court concludes that Exemptions 1, 3, and 7(E) independently apply to the requested information, and that Exemption 4 does not. Accordingly, as set forth below, the FBI's motion for summary judgment is GRANTED, and Plaintiffs' cross-motion for summary judgment is DENIED.

I. BACKGROUND

In December 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen people and injured twenty-two others in an attack on the Inland Regional Center in San Bernardino, California. *See* Government's Motion to Compel Apple Inc. to Comply, No. 5:16-cm-10-SP (C.D. Cal.) at 1 ECF No. 1. The FBI led the federal investigation into the attack, and during the course of that investigation, discovered an employer-owned iPhone issued to Farook that was password-protected. *See id.* at 1, 5. The phone was equipped with an auto-erase function that would result in the permanent destruction of the information in the phone after 10 failed attempts at entering the passcode. *Id.* at 5. Thus, the FBI was unable to access the phone without risking the loss of its contents. *Id.* at 10-11. After initially commencing legal action against the phone's manufacturer, Apple, to compel its assistance in accessing the phone, *id.* at 6, the FBI moved to stay the proceedings in March 2016 when an "outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone." Government's *Ex Parte* Application for a Continuance, No. 5:16-cm-10 (C.D. Cal.) at 3 ECF No. 191.

Rather than allow competitive bidding, the FBI sought a waiver to solicit a single source for the contract to unlock the phone. (Declaration of Jay Ward Brown ("Brown Decl.") Ex. J, at

AP-19–AP-23). None of the vendors who inquired with the agency about unlocking the phone had demonstrated that they could produce a solution quickly enough to meet the FBI's investigative requirements, and in fact, none of them had begun to develop or test a solution at the time of the inquiries. (*Id.* at AP-22). At the end of March 2016, the FBI reported that it had "successfully accessed the data stored on Farook's iPhone and therefore no longer require[d] the assistance from Apple Inc." Government's Status Report, No. 5:16-cm-10 (C.D. Cal.) at 1 ECF No. 209.

Following this revelation, then-FBI Director James Comey gave interviews to reporters on April 21, 2016, and May 11, 2016, during which he confirmed several details regarding the tool and its purchase. (Brown Decl. Ex. G; Ex. H; Ex. I). This information included details about its cost, which Comey believed "for sure" exceeded the salary he was due at the time for the remainder of his seven-year, four-month tenure, about $1.2 million. (Brown Decl. Ex. G). He also stated that the tool was narrowly tailored to only work on an iPhone 5C operating on iOS 9, and the FBI had not identified any other phones on which the tool could be used. (Brown Decl. Ex. I at 3, 16). Moreover, he noted that the urgency of the FBI's investigation necessitated the FBI's purchase of the tool and the agency spent what it needed to in order to acquire it. (*Id.* at 5).

Each Plaintiff filed a separate FOIA request with the FBI between March and April of 2016. (*See* Declaration of David M. Hardy ("First Hardy Decl.") Ex. A; Ex. I; Ex. M). They sought records concerning the FBI's financial agreements with the vendor the agency employed to unlock the iPhone. (*See id.*) The FBI initially denied each request on the basis of FOIA Exemption 7(A), which permits agencies to withhold records or information compiled for law enforcement purposes to the extent that the production of such records could reasonably be

expected to interfere with law enforcement proceedings. (First Hardy Decl. Ex. C; Ex. J; Ex. N). Each Plaintiff appealed administratively as provided under FOIA, and the Department of Justice Office of Information Policy affirmed the FBI's denial of the requests for the records in each case. (First Hardy Decl. Ex. D; Ex. H; Ex. K; Ex. L; Ex. O; Ex. Q).

Plaintiffs then filed this action in September 2016. (ECF No. 1). On January 6, 2017, the FBI produced 100 of 123 responsive pages in full or in part, with certain information withheld or redacted pursuant to FOIA Exemptions 1, 3, 4, 6, 7(C), and 7(E). (First Hardy Decl. ¶ 25; Ex. R; Brown Decl. Ex. J). The FBI then moved for summary judgment (ECF No. 14), and Plaintiffs filed their cross-motion for summary judgment, narrowing their outstanding FOIA request to two pieces of information: (1) the identity of the vendor, and (2) the amount paid to the vendor for the tool in question. (*See* Pls. Mem at 9, ECF Nos. 15, 16). As a result of this revised request, the remaining issues on summary judgment are whether the FBI properly applied Exemptions 1, 3, and 7(E) to the identity of the vendor, and whether it properly applied Exemptions 1, 3, 4, and 7(E) to the purchase price.

II. PLAINTIFFS' MOTION TO SUPPLEMENT THE RECORD

On May 3, 2017, Director Comey testified before the Senate Judiciary Committee. (*See* Supplemental Declaration of Jay Ward Brown "Supp. Brown Decl." Ex. A). During questioning, Senator Dianne Feinstein mentioned the FBI's hacking of Farook's iPhone, as excerpted below from the hearing transcript:

> FEINSTEIN: Well I – I was so struck when San Bernardino happened and you made overtures to allow that device to be opened, and then the FBI had to spend $900,000 to hack it open. And as I subsequently learned of some of the reason for it, there were good reasons to get into that device.
>
> And the concern I have is that once people had been killed in a terrorist attack and that there may be other DNA, there may be other messages that lead an investigative agency

> to believe that there are others out there, isn't to the – for the protection of the public that one would want to be able to see if a device could be opened.
>
> And I've had a very hard time – I've tried – I've gone out, I tried to talk to the tech companies that are in my state. One – Facebook was very good and understood the problem. But most do not have. Has the FBI ever talked with the tech companies about this need in particular?
>
> COMEY: Yes, senator. We've had a lot of conversations, and as I said earlier, they're – in my sense, they've been getting more productive because I think the tech companies have come to see the darkness a little bit more. My – my concern was privacy's really important but that they didn't see the public safety costs.
>
> I think they're starting to see that better and what – what nobody wants to have happen is something terrible happen in the United States and it be connected to our inability to access information with lawful authority. That we ought to have the conversations before that happens and the companies more and more get that. I think over the last year and half, and – but it's vital, we weren't picking on Apple in the San Bernardino case.

(*Id* at 4). On May 12, 2017, Plaintiffs moved to supplement the record on summary judgment with this testimony, citing it as "further evidence in support of [their] arguments on pages 15, 20, 26, and 29" of their memorandum in support of their cross-motion. (ECF No. 20 at 2).

Regarding Exemption 1, Plaintiffs note that then-Director Comey has already spoken publicly about the price (namely that it was very high), and thus disclosing the price information would not jeopardize national security interests. (*See* Pls. Mem. at 15). Regarding Exemption 3, Plaintiffs claim the FBI's argument that releasing the specific purchase price would aid those seeking to thwart the FBI's tool is belied by the fact that the information that could provide such aid—that the purchase price was very high—is already publicly available. (*See id.* at 20). Regarding Exemption 4, Plaintiffs emphasize that the tool's vendor would not suffer competitive harm from disclosure of the purchase price because Comey already released the general price-related information, and potential competitors have a ballpark figure from which to underbid. (*See id.* at 26). Regarding Exemption 7(E), Plaintiffs argue that releasing the purchase price will

not risk circumvention of the law because the FBI took that risk when Director Comey revealed that the purchase price was substantial. (*See id.* at 29).

The court will GRANT Plaintiffs' motion to supplement the record with the Senate Judiciary Committee hearing transcript, and will consider it part of Plaintiffs' brief in the sections detailed above.

III. SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate where the record shows there is no genuine issue of material fact and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Waterhouse v. District of Columbia*, 298 F.3d 989, 991 (D.C. Cir. 2002). In determining whether a genuine issue of material fact exists, the court must view all facts in the light most favorable to the non-moving party. *See, e.g.*, *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 157 (1970). A fact is material if "a dispute over it might affect the outcome of a suit under governing law; factual disputes that are 'irrelevant or unnecessary' do not affect the summary judgment determination." *Holcomb v. Powell*, 433 F.3d 889, 895 (D.C. Cir. 2006) (quoting *Anderson v. Liberty Lobby*, 477 U.S. 242, 248 (1986)). An issue is genuine if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* (quoting *Anderson*, 477 U.S. at 248). The party seeking summary judgment "bears the heavy burden of establishing that the merits of his case are so clear that expedited action is justified." *Taxpayers Watchdog, Inc., v. Stanley*, 819 F.2d 294, 297 (D.C. Cir. 1987).

FOIA cases are typically and appropriately decided on motions for summary judgment. *Brayton v. Office of the U.S. Trade Rep.*, 641 F.3d 521, 527 (D.C. Cir. 2011). Agencies bear the burden of justifying withholding of any records, as FOIA favors a "strong presumption in favor

of disclosure." *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991). The court therefore analyzes all underlying facts and inferences in the light most favorable to the FOIA requester, even where the requester has moved for summary judgment. *See Pub. Citizen Health Research Grp. v. FDA*, 185 F.3d 898, 904–05 (D.C. Cir. 1999).

In cases where the applicability of certain FOIA exemptions is at issue, agencies may rely on supporting declarations that are reasonably detailed and non-conclusory. *See, e.g., ACLU v. U.S. Dep't of Def.*, 628 F.3d 612, 619 (D.C. Cir. 2011); *Students Against Genocide v. Dep't of State*, 257 F.3d 828, 838 (D.C. Cir. 2001). "If an agency's affidavit describes the justifications for withholding the information with specific detail, demonstrates that the information withheld logically falls within the claimed exemption, and is not contradicted by contrary evidence in the record or by evidence of the agency's bad faith, then summary judgment is warranted on the basis of the affidavit alone." *ACLU*, 628 F.3d at 619. "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Id.* (internal quotation marks omitted) (quoting *Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009)). However, a motion for summary judgment should be granted in favor of the FOIA requester where "an agency seeks to protect material which, even on the agency's version of the facts, falls outside the proffered exemption." *Coldiron v. U.S. Dep't of Justice*, 310 F. Supp. 2d 44, 48 (D.D.C. 2004) (quoting *Petroleum Info. Corp. v. Dep't of Interior*, 976 F.2d 1429, 1433 (D.C. Cir. 1992)).

IV. DISCUSSION

The defendant in a FOIA case must show that its search for responsive records was adequate, that any claimed exemptions are valid, and that any reasonably segregable non-exempt

portions of records have been disclosed after redaction of exempt information. *Light v. Dep't of Justice*, 968 F. Supp. 2d 11, 23 (D.D.C. 2013).

Here, Plaintiffs have conceded that the FBI's search for responsive records was adequate, and do not challenge the FBI's segregability determination. They do, however, contest the FBI's claimed exemptions for the tool vendor's identity and the tool's purchase price. The FBI asserts that such information is properly and independently protected under FOIA Exemptions 1, 3, and 7(E), and that the purchase price is also independently protected under FOIA Exemption 4. (Def. Opp. at 1). For the reasons set forth below, the court finds that Exemptions 1, 3, and 7(E) apply to both the vendor's identity and the purchase price, and Exemption 4 does not apply to the purchase price. Although invocation of a single valid exemption is sufficient to permit the withholding of the information requested and support a grant of summary judgment to the FBI, the court will nevertheless analyze the application of each exemption.

A. FOIA Exemption 1

1. Applicable Legal Standard

FOIA Exemption 1 protects from disclosure records that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). Executive Order 13,526 currently governs the classification of national security information, and requires that:

> (1) an original classification authority is classifying the information;
>
> (2) the information is owned by, produced by or for, or is under the control of the United States Government;
>
> (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Classified National Security Information, EO 13,526 § 1.1(a); 75 Fed. Reg. 707 (2009). Plaintiffs do not dispute that the FBI has met the first and second requirements, (*see* Pls. Mem. at 12-18), as the Hardy Declaration demonstrates that Hardy is an original classification authority and that the withheld information is under the control of the United States Government. (First Hardy Decl. ¶ 2, 33). The FBI asserts that the third requirement is satisfied because the identity of the vendor and the cost of the tool relate to intelligence activities or intelligence sources or methods under Section 1.4(c) of the Executive Order. (First Hardy Decl. ¶ 33) (citing Exec. Order No. 13,526 § 1.4(c); 75 Fed. Reg. at 708). Plaintiffs do not appear to challenge this assertion. (*See* Pls. Mem. at 12-18; Pls. Reply at 2-5, 7-11).

The parties' dispute involves the fourth requirement, which permits withholding if the information requested could reasonably be expected to cause an identifiable and describable degree of harm to national security if released. *Judicial Watch, Inc. v. Dep't of Def.*, 715 F.3d 937, 941 (D.C. Cir. 2013). The court owes "substantial weight" to detailed agency explanations in the national security context; its role is to ensure that the government's rationale is logical or plausible. *Id.* at 941, 943; *see also Judicial Watch, Inc. v. Dep't of Commerce*, 337 F. Supp. 2d 146, 162 (D.D.C. 2004) ("In light of courts' presumed lack of expertise in the area of national security, a reviewing court is prohibited from conducting a detailed analysis of the agency's invocation of Exemption 1." (citing *Halperin v. CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980))). Further, "the text of Exemption 1 suggests that little proof or explanation is required beyond a plausible assertion that information is properly classified." *Morley v. CIA*, 508 F.3d 1108, 1124 (D.C. Cir. 2007). However, conclusory affidavits that merely recite statutory standards, or that

are overly vague or sweeping, will not suffice to carry the government's burden. *Larson*, 585 F.3d at 864.

2. Whether the FBI Properly Invoked Exemption 1 with Respect to the Vendor's Identity

The FBI argues that releasing the vendor's identity could allow adversaries to use existing public technology created by the vendor to probe for weaknesses and create better encryption technology to thwart the FBI's ability to use the tool. (Second Declaration of David M. Hardy ("Second Hardy Decl.") ¶ 8-9). The agency argues that because software companies "update and modernize their old operating systems rather than create a completely new product," there are programming styles and strategies unique to most companies, likely including the vendor at issue. (*Id.* ¶ 8). Thus, if the vendor's identity were made public, a review of the company's work could lead antagonists to "develop exploits for the vendor's unique product." (*Id.*) Additionally, the FBI notes that because the vendor's networks are not as sophisticated as the FBI's cyber-security facilities, releasing the name of the vendor could subject the vendor to attacks by entities who wish to exploit the technology. (*Id.* ¶ 9). Since the vendor is not as well equipped to guard against these types of attacks as is the FBI, revealing the vendor's identity "risks disclosure, exploitation, and circumvention of a classified intelligence source and method." (*Id.*) Disclosure of the vendor's identity could thus "reasonably be expected to cause serious damage to national security, as it would allow hostile entities to discover the current intelligence gathering methods used, as well as the capabilities and limitations of those methods." (First Hardy Decl. ¶ 36).

This line of reasoning logically and plausibly demonstrates how the FBI could reasonably expect the release of the vendor's identity to cause identifiable harm to national security. If an adversary were determined to learn more information about the iPhone hacking tool the FBI

acquired, it is certainly logical that the release of the name of the company that created the tool could provide insight into the tool's technological design. Adversaries could use this information to enhance their own encryption technologies to better guard against this tool or tools the vendor develops for the FBI in the future. Plaintiffs assert that it is unlikely that a public body of work which an adversary could use even exists, (Pls. Reply at 3), given that the vendor is likely sophisticated enough to avoid risking the usefulness of its technology by making such work available, but it is plausible that useful information about a software company's technological design could be gleaned from its other publicly available products.

Moreover, it is logical and plausible that the vendor may be less capable than the FBI of protecting its proprietary information in the face of a cyber-attack. The FBI's conclusion that releasing the name of the vendor to the general public could put the vendor's systems, and thereby crucial information about the technology, at risk of incursion is a reasonable one. Plaintiffs here assume that this is not a legitimate threat, and that if the tool were so critically important to national security, the FBI would not have left it in the hands of a "poorly guarded vendor." (Pls. Reply at 4 n.1). But the vendor may continue to possess the tool for any number of reasons related to national security interests, and even if the possibility of an attack on the vendor's systems is remote, the FBI has still demonstrated a logically reasonable risk of harm to national security in this respect.

The court therefore finds that the FBI has shown that the release of the vendor's identity could be reasonably expected to cause harm to national security interests by limiting the FBI's present and future ability to gain access to suspected terrorists' phones. Although as of May 2016 the FBI had not yet identified other phones with which the tool could be utilized, (Brown Decl. Ex. I at 3), any affidavit describing a potential threat to national security "will always be

speculative to some extent." *ACLU*, 628 F.3d at 619. There is no evidence to suggest that the tool will not be valuable in the future, and the FBI has met its burden of providing a detailed, non-conclusory affidavit sufficient to invoke Exemption 1 as applied to the vendor's identity.

Plaintiffs argue that Director Comey's public comments about the tool's efficacy negate the risk that an adversary will attempt to learn more about it, since the route to developing a countermeasure seems fairly straightforward. (Pls. Mem. at 15-16). After Director Comey emphasized that he was "highly confident" that the tool only works on iPhone 5Cs running iOS9 (Brown Decl. Ex. I at 16), any organization intending to prevent the FBI from using the tool to hack its members' phones could therefore use a different phone or a different operating system. However, this overlooks the tool's potentially valuable technical capabilities. The FBI may find a way to enhance the tool's capabilities, choose to continue using advanced versions of similar technology in the future, or re-employ the vendor to develop another similar product. It is certainly plausible that disclosure of the vendor's name could hurt the FBI's future efforts to protect national security, despite opportunities to circumvent the tool that may arise from Comey's comments. The FBI therefore properly invoked Exemption 1 with respect to the vendor's identity.

3. Whether the FBI Properly Invoked Exemption 1 with Respect to the Purchase Price

The FBI argues that revealing the price paid for the tool would allow adversaries to determine its usefulness and assess its nature, and would reveal where the FBI concentrates its resources in national security investigations. (Second Hardy Decl. ¶ 16-18). Releasing the purchase price would designate a finite value for the technology and help adversaries determine whether the FBI can broadly utilize the technology to access their encrypted devices. (*Id.* ¶ 16). Since release of this information might "reduce the effectiveness of a critical classified source

and method," it is reasonable to expect that disclosure could endanger national security. (*Id.* ¶ 19).

The court finds that the Second Hardy Declaration logically and plausibly sets forth how the release of the purchase price could cause a reasonably expected risk of harm to national security. "Minor details of intelligence information," like the price paid for the iPhone hacking tool, "may reveal more information than their apparent insignificance suggests because, much like a piece of jigsaw puzzle, each detail may aid in piecing together other bits of information." *Leopold v. CIA*, 106 F. Supp. 3d 51, 59 (D.D.C. 2015) (quoting *Larson*, 565 F.3d at 864) (internal quotation marks omitted). The price the FBI paid for the tool could logically reveal how much the FBI values gaining access to suspects' phones, and the breadth of the tool's capabilities. Accordingly, the FBI has met its burden of providing a detailed, non-conclusory affidavit sufficient to invoke Exemption 1 with respect to the purchase price.

Plaintiffs argue that Director Comey's public comments about the purchase price negate the possibility of any further harm to national security. (Pls. Mem. at 15). Because he has already disclosed the "only possible useful bit of information about the tool's price, namely, that it was very high," they argue that there is no justification for withholding the exact price. (*Id.*) They further note that the agency's national security priorities have already been made clear by virtue of Comey's statement that the government will pay "what is necessary," (Brown Decl. Ex. I at 5), to access suspected terrorists' phones. (Pls. Reply at 10). However, Plaintiffs fail to address this Circuit's test for when an agency's official disclosure may compel release of otherwise valid exemption claims. Although it is true that "when information has been officially acknowledged, its disclosure may be compelled even over an agency's otherwise valid

exemption claim" *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990), the claim must meet the following "strict test":

> To be officially disclosed: (1) the information requested must be as specific as the information previously released; (2) the information requested must match the information previously disclosed; and (3) the information requested must already have been made public through an official and documented disclosure. Thus, a plaintiff asserting a claim of prior disclosure must bear the initial burden of pointing to specific information in the public domain that appears to duplicate that being withheld.

Moore v. CIA, 666 F.3d 1330, 1333 (D.C. Cir. 2011) (internal citations omitted). Since this court has found that the FBI's invocation of Exemption 1 with respect to the purchase price is valid, Director Comey's public comments must meet the requirements set forth in *Moore* in order to compel disclosure of the purchase price. The comments fail the first requirement—Comey provided only a general estimate, rather than the specific price paid for the tool. He admitted himself that in making that estimate, he was "just winging that." (Brown Decl. Ex. I at 2).

Plaintiffs' supplemental evidence fares no better. (*See* Supp. Brown Decl. Ex. A at 2). Even if Senator Feinstein was correct that the FBI paid $900,000 for the tool, Director Comey did not acknowledge or verify Sen. Feinstein's comment, and Comey's testimony therefore fails the third element of the test, since the information was not made public through an *agency's* official disclosure.

Plaintiffs also insist that the FBI seeks to prevent disclosure of the purchase price in order to prevent embarrassment and restrain competition, not to protect national security, in violation of section 1.7(a) of Executive Order 13,526; 75 Fed. Reg. at 710. Plaintiffs' allegation is based on Comey's comment that he would not disclose the exact purchase price, stating "I don't want to waste your tax payers [sic] money." (Brown Decl. Ex. I at 11). However, Plaintiffs ignore the context in which this statement was made. It appears Comey was attempting to explain that he did not want to reveal the purchase price because he did not wish to hurt the FBI's negotiating

position the next time a similar tool was purchased, thus potentially saving public funds. (*See* Brown Decl. Ex. I at 10-11). This comment does not reveal any desire to prevent embarrassment to the FBI, and Plaintiffs provide no evidence for their conclusory statement that withholding the purchase price will "artificially alter[] the competitive landscape for technology contracting." (Pls. Mem. at 15). This single statement from the former FBI Director is an insufficient basis for this court to determine that the FBI's motive for withholding the purchase price is improper. Plaintiffs must provide something more than conjecture to show that the agency's withholding decision violates Executive Order 13,526. *See Canning v. Dep't of Justice*, 848 F. Supp. 1037, 1048 (D.D.C. 1994). They have failed to do so.

Despite Comey's assertions about the price the FBI paid for the tool, his statements do not amount to an official disclosure that compels the release of the information over the agency's valid exemption claim, and there is no evidence that the FBI has an improper motive in invoking the exemption. The agency has provided a logical and plausible affidavit that adequately demonstrates how the release of the purchase price could cause a reasonably expected risk of harm to national security, and thus they have properly invoked Exemption 1 with respect to the purchase price.

B. FOIA Exemption 3

1. Applicable Legal Standard

FOIA Exemption 3 protects from disclosure information that has been specifically exempted by statute, if that statute "(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3)(A). Courts apply a two-pronged inquiry when evaluating Exemption 3 invocations, first determining

whether the statute is an exempting statute, and then evaluating whether the requested material falls within the scope of that statute. *CIA v. Sims*, 471 U.S. 159, 167 (1985). Here, the FBI relies on section 102A(i)(1) of the National Security Act of 1947 (the "Act"), which protects intelligence sources and methods from unauthorized disclosure. 50 U.S.C. § 3024(i)(1). Plaintiffs do not dispute that the Act qualifies as an exempting statute for the purpose of Exemption 3. (Pls. Mem. at 18); *ACLU*, 628 F.3d at 619. Accordingly, the issue here is whether the withheld information protects intelligence sources and methods.

This Circuit has interpreted the Act "broadly," holding that material is exempt if it relates to intelligence sources and methods, or can reasonably be expected to lead to the unauthorized disclosure of intelligence sources and methods. *Leopold*, 106 F. Supp. 3d at 57 (citing *Larson*, 565 F.3d at 865; *Halperin*, 629 F.2d at 147). The exemption includes the "power to withhold superficially innocuous information on the ground that it might enable an observer to discover the identity of an intelligence source or method." *Id.* (quoting *Sims*, 471 U.S. at 178). The Act presents an easier hurdle for the agency under Exemption 3 than does Executive Order 13,526 under Exemption 1, in that it does not require the FBI to determine that release of the information could reasonably be expected to result in damage to national security. *See* 50 U.S.C. § 3024(i)(1).[1]

[1] Plaintiffs' challenge of the FBI's invocation of Exemption 3 is inconsistent with their challenge of Exemption 1. They do not appear to contest that the information they seek pertains to intelligence sources or methods under Section 1.4(c) of Executive Order 13,526, (*see* Pls. Mem. at 12-18; Pls. Reply at 2-5, 7-11), but they later contend that it does not "actually relate" to intelligence sources or methods under the Act. (Pls. Mem. at 19) (citing *Larson*, 565 F.3d at 865). These two positions do not appear reconcilable.

2. Whether the FBI Properly Invoked Exemption 3 with Respect to the Vendor's Identity

The FBI considers the iPhone hacking tool itself to be an intelligence source and method, (Second Hardy Decl. ¶ 8), and the court agrees. The tool allows the FBI to access intelligence information on suspects' phones, therefore logically serving as both a source of intelligence information and method for obtaining intelligence information. The FBI argues that release of the vendor's identity relates to an intelligence source and method because it could lead to information about the tool, in the same manner as discussed under Exemption 1. (*Id.* ¶ 8-9). For the reasons set forth in Section III.A.2, *supra*, the court finds that this is an adequate justification for withholding the vendor's identity pursuant to Exemption 3.

Plaintiffs argue that the FBI's position is undercut because it did not claim that the vendor's identity was an intelligence source. (Pls. Mem. at 20). But this fact is irrelevant under the legal standard, as Plaintiffs acknowledge—the information requested must only *relate* to intelligence sources or methods. *Larson*, 565 F.3d at 865. Plaintiffs also claim that the FBI's assertion that releasing the vendor's identity could allow an adversary to learn more about the tool's capabilities is speculative, arguing that the FBI "has identified no rational reason why knowing the vendor's identity is linked in any way to the substance of the tool, much less how such knowledge would reveal any information about the tool's application[.]" (Pls. Mem. at 20). However, as the court previously noted, any affidavit that describes a threatened harm to national security "will always be speculative to some extent," *ACLU*, 628 F.3d at 619, and the FBI has shown how the vendor's identity logically relates to an intelligence source and method. Accordingly, the FBI properly invoked Exemption 3 with respect to the vendor's identity.

3. Whether the FBI Properly Invoked Exemption 3 with Respect to the Purchase Price

The FBI argues that information regarding the purchase price relates to an intelligence source and method because it could lead to information about the iPhone hacking tool, in the same manner as discussed under Exemption 1. (Second Hardy Decl. ¶ 16-18). For the reasons set forth in Section III.A.3, *supra*, the court finds that this is an adequate justification for withholding the purchase price pursuant to Exemption 3.

Plaintiffs' argument again centers on Director Comey's public statements about the tool's purchase price, asserting that all relevant information about the price has already been released. (Pls. Reply at 9-11). As the court previously discussed in Section III.A.3, *supra*, Comey's comments did not constitute an official disclosure such that the release of the purchase price could be compelled over the FBI's valid exemption claim. Accordingly, the FBI properly invoked Exemption 3 with respect to the tool's purchase price.

C. FOIA Exemption 7(E)

1. Applicable Legal Standard

FOIA Exemption 7(E) protects from disclosure "records or information compiled for law enforcement purposes" when production of such records "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). To fall within Exemption 7, information must first meet a threshold requirement: that the records were compiled for law enforcement purposes. *Pub. Emps. for Envtl. Responsibility ("PEER") v. U.S. Section, Int'l Boundary & Water Comm'n*, 740 F.3d 195, 202-03 (D.C. Cir. 2014). Here, this threshold is clearly met; Plaintiffs do not dispute that the FBI compiled the withheld information for law

enforcement purposes, (Pls. Mem. at 28-31), and that the records related to the vendor were clearly compiled to further the law enforcement investigation into the San Bernardino terrorist attack.

Although courts are divided over whether the "risk circumvention of the law" requirement applies to techniques and procedures as well as guidelines, this Circuit has applied the requirement to records containing techniques and procedures as well as those containing guidelines. *PEER*, 740 F.3d at 204 n.4 (citing *Blackwell v. FBI*, 646 F.3d 37, 41-42 (D.C. Cir. 2011)). The FBI acknowledges this is the proper test here. (*See* Second Hardy Decl. ¶ 11). Still, Exemption 7(E) "sets a relatively low bar for the agency to justify withholding." *Blackwell*, 646 F.3d at 41. As the court in *Mayer Brown LLP v. IRS* put it,

> the exemption looks not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk.

562 F.3d 1190, 1193 (D.C. Cir. 2009). The exemption does not require a specific showing of how the law will be circumvented, only that the agency demonstrate logically how the release of the requested information might create a risk of circumvention. *Id.* at 1194; *see also Blackwell*, 646 F.3d at 42.

2. Whether the FBI Properly Invoked Exemption 7(E) with Respect to the Vendor's Identity

The FBI argues that, as a law enforcement agency, it could use the iPhone unlocking technology in future law enforcement activities, making the iPhone hacking tool itself a law enforcement technique. (Second Hardy Decl. ¶ 10). The court agrees. Although the vendor's identity is itself not a law enforcement technique, the FBI contends that disclosing the vendor's identity will allow hostile entities to discover how the iPhone hacking tool works and then use

that information to circumvent the technology in the same manner this court found to be logical and plausible under Exemption 1 in Section III.A.2, *supra*. Bearing in mind that the FBI must only show that release of the information will create a "chance of a reasonably expected risk" of circumvention of the law, *Mayer Brown*, 562 F.3d at 1193, the agency has met its burden to show that it properly invoked Exemption 7(E).

Plaintiffs argue once again that there is no risk that revealing the vendor's identity will cause circumvention of the law, because the tool can already be circumvented by using a phone that is not an iPhone 5C or any operating system other than iOS9. (Pls. Mem. at 31). This overlooks the tool's potential value to the FBI in future iterations of the technology, and Plaintiffs themselves acknowledge that Exemption 7(E) presents a low bar for the agency. The FBI "has not publicly explained how the technology works," (Second Hardy Decl. ¶ 11), and releasing the vendor's identity could provide individuals with a recourse to discovering how to circumvent its use in the future. Accordingly, release of the vendor's identity would risk disclosure of a law enforcement technique and create a reasonably expected risk of circumvention of the law. Therefore, the FBI properly invoked Exemption 7(E) with respect to the vendor's identity.

3. Whether the FBI Properly Invoked Exemption 7(E) with Respect to the Purchase Price

The FBI argues that although the cost of a single contract is not a law enforcement technique or procedure, it must be considered in conjunction with the law enforcement technique to which it relates, namely, the iPhone hacking tool. (*Id.* ¶ 16). The FBI's posits that if the total price paid for the iPhone hacking tool were revealed, adversaries would be able to assess the nature of the tool and determine its likely capabilities. (*Id.* ¶ 17). The agency further asserts that revealing specific financial allotments for technology acquisition will disclose where the FBI

concentrates its resources for national security investigations, and that releasing non-public details like a purchase price could allow "potential targets to carefully put together building blocks of information that would result in the degradation of the effectiveness of [intelligence gathering] tools." (*Id.* ¶ 18). This in turn could give rise to the development of countermeasures by hostile entities that could cause circumvention of the law. (*Id.*) The court finds this explanation to be logical and plausible, and it meets Exemption 7(E)'s low bar for records that would reveal law enforcement techniques and risk circumvention of the law.

Plaintiffs again argue that these risks have already been created by Comey's public comments about the purchase price, and that because this "theory of harm is long since out of the barn," release of the purchase price would not create a further risk of circumvention of the law. (Pls. Mem. at 30). However, as discussed in Section III.A.3, *supra*, Comey's comments do not amount to an official disclosure that compels the release of requested information over the FBI's valid exemption claim. Accordingly, the FBI properly invoked Exemption 7(E) with respect to the purchase price.

D. FOIA Exemption 4

1. Applicable Legal Standard

FOIA Exemption 4 protects "trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). The purpose of this exemption is to "balance the strong public interest in favor of disclosure against the right of private businesses to protect sensitive information." *Nat'l Parks & Conservation Ass'n v. Morton* ("*Nat'l Parks I*"), 498 F.2d 765, 768-69 (D.C. Cir. 1974).

In order to qualify for withholding under Exemption 4, information withheld must "(1) involve trade secrets or commercial or financial information; (2) be obtained from a person

outside the government; and (3) be privileged or confidential." *Biles v. Dep't of Health & Human Servs.*, 931 F. Supp. 2d 211, 219 (D.D.C. 2013) (citing *Nat'l Parks I*, 498 F.2d at 766); *see also CREW v. U.S. Dep't of Justice*, 160 F. Supp. 3d 226, 237 (D.D.C. 2016) (citing *Pub. Citizen Health Research Grp. v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983)). Plaintiffs do not dispute that the purchase price paid to the vendor qualifies as commercial or financial information, or that it was obtained from a person outside the government. The FBI does not assert that the purchase price is privileged, so the sole issue before the court here is whether the price is confidential.

The court must first decide whether the purchase price constitutes material that was submitted to the government voluntarily, or material that the government required to be submitted. *Biles*, 931 F. Supp. 2d at 219-20 (citing *Critical Mass Energy Project v. NRC*, 975 F.2d 871, 878-80 (D.C. Cir. 1992) (en banc)). Information that an entity is required to provide is less rigorously protected than information it voluntarily provides to the government. *Id.* at 219. The parties here agree that information submitted for a government contract is an involuntary submission. (Def. Mem. at 16; Pls. Mem. at 22); *see McDonnell Douglas Corp. v. Dep't of the Air Force*, 375 F.3d 1182, 1187 (D.C. Cir. 2004). When information is required to be submitted to the government, it is considered confidential under FOIA if "disclosure is likely ... (1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained." *Nat'l Parks I*, 498 F.2d at 770. The FBI argues that its invocation of Exemption 4 is appropriate under either prong.

2. Whether Disclosure of the Purchase Price is Likely to Impair the FBI's Ability to Obtain Necessary Information in the Future

The FBI contends that disclosing the purchase price may dissuade future contractors from working with the FBI, for fear that the FBI would publicize information about their own financial transactions. (First Hardy Decl. ¶ 46; Second Hardy Decl. ¶ 15). However, whether an entity will *participate* in a government program is not relevant in deciding whether the government will be impaired in its ability to obtain information in the future from those entities that *do* participate. "Where the government obtains information involuntarily, disclosure does not impair the government's ability to obtain similar information in the future." *In Def. of Animals v. Dep't of Agric.*, 656 F. Supp. 2d 68, 72 (D.D.C. 2009); *see also Martin Marietta Corp. v. Dalton*, 974 F. Supp. 37, 40 (D.D.C. 1997). Accordingly, the FBI's invocation of Exemption 4 with respect to the purchase price was not appropriate under the first prong of *National Parks I*.

3. Whether Disclosure of the Purchase Price is Likely to Cause Substantial Harm to the Competitive Position of the Vendor

Under the competitive injury prong, the FBI must establish that the vendor (1) actually faces competition, and (2) substantial competitive injury would likely result from disclosure. *Nat'l Parks and Conservation Ass'n v. Kleppe* (*Nat'l Parks II*), 547 F.2d 673, 679 (D.C. Cir. 1976). The competitive injury must "be limited to harm flowing from the affirmative use of the proprietary information *by competitors*." *Pub. Citizen Health Res. Grp.*, 704 F.2d at 1291 n.30 (emphasis in original). However, a "sophisticated economic analysis of the likely effects of disclosure" is not required. *Id.* at 1291 (citing *Nat'l Parks II*, 547 F.2d at 681). The agency need not "prove that substantial harm is 'certain' to result from disclosure, but only that such harm is 'likely.'" *Boeing v. Dep't of Air Force*, 616 F. Supp. 2d 40, 45 (D.D.C. 2009) (citing *McDonnell*

Douglas Corp., 375 F.3d at 1187). Further, the agency need only proffer evidence indicating the existence of potential competitive injury or economic harm. *Essex Electro Eng'rs, Inc. v. Sec'y of Army*, 686 F. Supp. 2d 91, 94 (D.D.C. 2010) (citing *Gulf & W. Indus., Inc. v. United States*, 615 F.2d 527, 530 (D.C. Cir. 1979)). Evidence of actual harm is not required. *Id.* However, the agency may not simply offer "conclusory and generalized allegations" of substantial competitive harm. *Nat'l Parks II*, 547 F.2d at 681. Instead, it must provide "specific factual or evidentiary material to support [its] claim that harm is likely to result." *Boeing*, 616 F. Supp. 2d at 45 (citing *Nat'l Parks II*, 547 F.2d at 679).

a. *Whether the Vendor Actually Faces Competition*

A sole source contract does not preclude a finding of actual competition. *Gen. Elec. Co. v. Dep't of the Air Force*, 648 F. Supp. 2d 95, 103 (D.D.C. 2009). The agency need not provide evidence of actual competition for the particular contract, only evidence of actual competition for future contracts. *Id.*

The FBI argues that because the vendor has proved that unlocking these devices is possible, it is reasonable to assume that the vendor's success will create future competition. (Second Hardy Decl. ¶ 14). However, in *General Electric*, the company demonstrated actual competition—its competitors were actively producing the parts covered by the relevant government contracts. Here, the FBI has not shown that any other vendor is even capable of producing a similar product, much less that one is actively attempting to do so. They merely speculate that there would be competition if the FBI were to request a similar tool in the future. (*See* Brown Decl. Ex. J at AP-22). Since there is no evidence that any actual competition exists over current or future contracts, the FBI has failed to demonstrate that the vendor actually faces

competition. Accordingly, the FBI's invocation of Exemption 4 was also not appropriate under the second prong of *National Parks I*.

b. *Whether Substantial Competitive Injury is Likely to Result From Disclosure of the Purchase Price*

Even if the FBI's assertion about potential future competition was sufficient to show actual competition, disclosure of the purchase price would be unlikely to cause substantial competitive injury. The FBI argues that releasing this information would grant potential government contractors an opportunity to judge how they might underbid the vendor in the future, hurting the vendor's ability to obtain government contracts. (First Hardy Decl. ¶ 45; Second Hardy Decl. ¶ 14). But the bidding process for this particular contract was unique and unlikely to be replicated. The contract price was based on time constraints caused by the urgency of the investigation and the vendor's ability to produce the tool quickly. Any future price paid for a similar contract in competitive bidding would likely be unaffected by the price paid here, as it reflected the unusual circumstances surrounding the investigation. Accordingly, the disclosure of the purchase price is unlikely to cause substantial competitive injury to the vendor.

The agency argues that its determination of substantial competitive injury is entitled to deference, but deference is only granted under Exemption 4 in a "reverse FOIA" case in which the plaintiff is challenging the agency's impending release of information. *Ctr. for Pub. Integrity v. Dep't of Energy*, 191 F. Supp. 2d 187, 196 (D.D.C. 2002) ("The rationale for showing deference in such cases is that… if the agency is willing to release information, it can be safely assumed that the agency is acting to protect its ability to contract in the future. This rationale clearly does not apply where an agency is withholding information"); *see also Jurewicz v. Dep't of Agric.*, 741 F.3d 1326, 1330-31 (D.C. Cir. 2014).

In sum, the court finds that disclosure of the purchase price (1) will not impair the FBI's ability to obtain similar information in the future, and (2) is not likely to cause substantial competitive harm to the vendor, because the vendor does not face actual competition, and even if it did, would not likely suffer competitive injury from disclosure. Accordingly, the purchase price is not confidential within the meaning of Exemption 4, and the FBI's application of the exemption to the purchase price was improper.

V. CONCLUSION

For the foregoing reasons, Plaintiffs' motion to supplement the record will be GRANTED; the FBI's motion for summary judgment will be GRANTED; and Plaintiffs' cross-motion for summary judgment will be DENIED.

A corresponding order will issue separately.

Dated: September 30, 2017

Tanya S. Chutkan
TANYA S. CHUTKAN
United States District Judge

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu