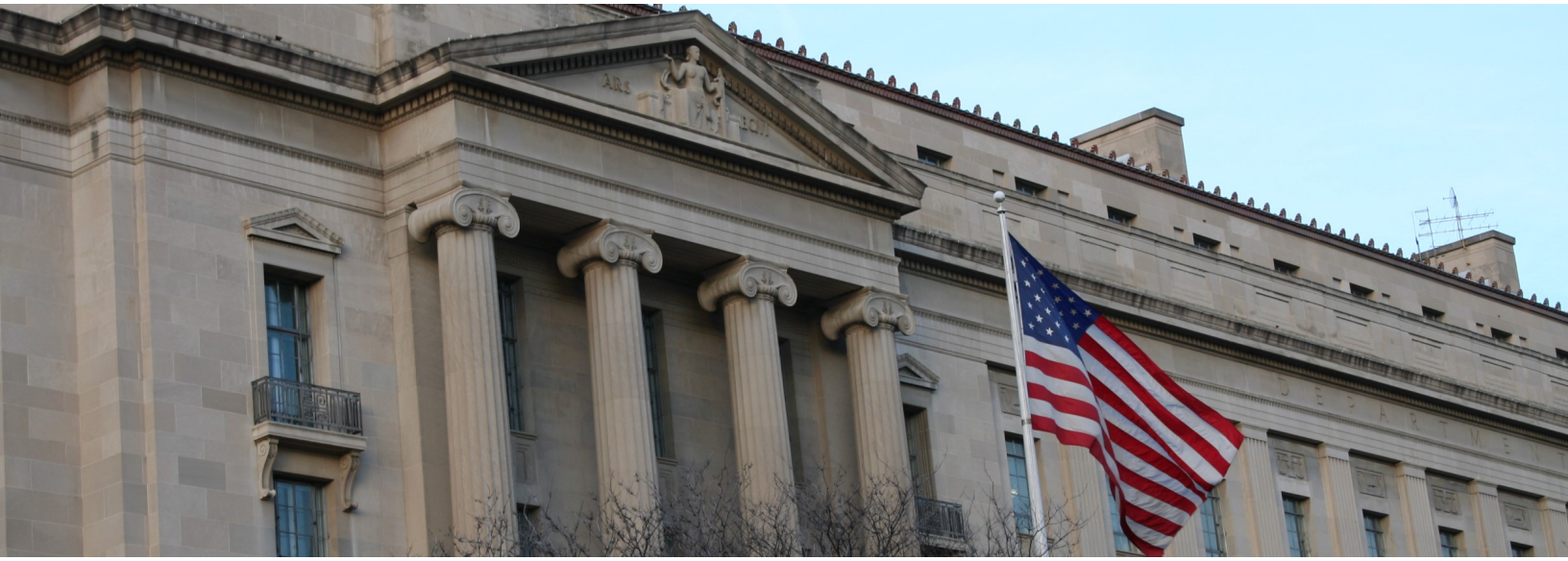
Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation

Oversight and Review Division 18-03

March 2018

Table of Contents

I. Background

On December 2, 2015, a terror attack in San Bernardino, California killed 14 people and injured 17 others. The next day, the Federal Bureau of Investigation (FBI) seized pursuant to a search warrant the iPhone of one of the subjects believed to have been responsible for the attack, Syed Rizwan Farook. Thereafter, on February 9 and March 1, 2016, then-FBI Director James Comey testified before Congress, in substance, that the FBI was not able to obtain access to data on the Farook iPhone, and then that it would require assistance from the manufacturer, Apple, to do so.[1] To accomplish this, on February 16, 2016, the U.S. Attorney's Office for the Central District of California (USAO) sought and obtained an *ex parte* court order requiring Apple to assist the FBI in its effort to search the iPhone. A few days later, the USAO filed a motion with the Court seeking to compel Apple's compliance with the *ex parte* order, and Apple filed a motion to vacate the order. However, on March 21, 2016, before the District Judge ruled on these pending motions, the USAO reported to the Court that an outside party had demonstrated to the FBI a possible method for unlocking the iPhone. One week later, on March 28, 2016, the USAO reported back to the Court that the FBI had successfully accessed the iPhone and no longer required assistance from Apple. On April 19, 2016, then-FBI Executive Assistant Director (EAD) Amy Hess testified about the matter before Congress and cited rapidly changing technology as a reason the FBI was not able to exploit the iPhone without the assistance of a third party.[2]

On August 31, 2016, the Office of the Inspector General (OIG) received a referral from the FBI Inspection Division after former EAD Hess expressed concern about an alleged disagreement between units within the FBI Operational Technology Division (OTD) over the "capabilities available to the national security programs" to access the Farook iPhone following its seizure, and concerns that this may have resulted in her or Comey giving inaccurate testimony to Congress on the FBI's capabilities. Specifically, EAD Hess expressed concerns that an OTD unit may have had techniques available to exploit the Farook iPhone that certain unidentified OTD officials did not employ and that these officials were indifferent to the fact that FBI leadership and others were testifying to Congress, and filing affidavits in court, that the FBI had no such capability. The OIG has conducted inquiries into the

---

[1] James B. Comey, Director, Federal Bureau of Investigation, before the Select Committee on Intelligence, U.S. Senate, concerning "Worldwide Threats" (February 9, 2016), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing (accessed July 20, 2017), and before the Judiciary Committee, U.S. House of Representatives, concerning "The Encryption Tightrope: Balancing Americans' Security and Privacy" (March 1, 2016), https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy (accessed July 20, 2017).

[2] Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, before the Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, U.S. House of Representatives, concerning "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives" (April 19, 2016), https://energycommerce.house.gov/hearings-and-votes/hearings/deciphering-debate-over-encryption-industry-and-law-enforcement (accessed July 20, 2017).

situation, including interviewing relevant key participants, and found no evidence that OTD had the capability to exploit the Farook iPhone at the time of the Congressional testimony and initial court filings. We therefore determined that neither the Congressional testimony nor the submissions to the Court were inaccurate when made. However, we found that inadequate communication and coordination within OTD caused a delay in engaging all relevant OTD personnel in the search for a technical solution to the Farook iPhone problem, as well as the outside party that ultimately developed the method that unlocked the phone, issues that we learned the FBI has since taken steps to address.

II. Relevant FBI Organizational Structure

OTD is responsible for providing technical assistance and support to the FBI's intelligence, national security, and law enforcement operations. According to EAD Hess, the Division is made up of approximately [redacted] employees and contractors who are divided into [redacted] sections, each of which is further divided into [redacted] to [redacted] units. Among these, the Cryptographic and Electronic Analysis Unit (CEAU) is a unit within OTD's Digital Forensics and Analysis Section (DFAS) and has forensic examiners who assist the field with obtaining evidence on digital devices, primarily, but not exclusively, in support of criminal matters. The Remote Operations Unit (ROU) within OTD's Technical Surveillance Section (TSS) provides computer network exploitation capabilities in support of [redacted].

By the nature of their work, both CEAU and ROU have engineers and vendors who attempt to develop techniques that can exploit mobile devices, with legal authorities appropriate for the types of matters in which they are involved. Reflective of the nature of their responsibilities, CEAU typically works on [redacted] whereas ROU works primarily on [redacted].

III. Accuracy of FBI Statements Regarding the Farook iPhone

Our inquiries into this matter revealed that CEAU tried to assist the criminal investigators working on the San Bernardino investigation by attempting to identify a technique that would allow the FBI to access the data inside the Farook iPhone. As reflected in the affidavit that the USAO originally submitted in support of the application for a court order, the Farook phone was an iPhone 5c running on Apple's iOS 9 operating system. At the time it was seized, the Farook iPhone was secured with a user-created numeric passcode and other security features on the iOS operating system (primarily the auto-erase function after 10 failed passcode attempts and the delay-upon-failure function) that made FBI investigators unable to employ previously known techniques to unlock the phone without risking the permanent destruction of potentially critical data. CEAU's efforts to overcome or bypass these security features were not successful, as reflected in the testimony by former Director Comey and the filing by the USAO referenced above.

The ROU Chief told us that, at a monthly OTD managers' meeting on February 11, 2016, the Chief of DFAS (of which CEAU is a part but ROU is not), indicated that CEAU was having problems accessing the data on the Farook iPhone and was preparing for court. The ROU Chief, who told the OIG that his unit did not have a technique for accessing the iPhone at the time, said that it was only after this meeting that he started contacting vendors and that ROU "got the word out" that it was looking for a solution. As discussed further below, at that time, he was aware that one of the vendors that he worked closely with was almost 90 percent of the way toward a solution that the vendor had been working on for many months, and he asked the vendor to prioritize completion of the solution.

According to the ROU Chief, on a date that we have determined to have been March 16, 2016, one of the outside vendors utilized by ROU came forward with a possible solution. The vendor successfully demonstrated the technique to FBI leadership on March 20, 2016, and the USAO notified the Court of this development the following day, requesting a continuance of a previously scheduled hearing. One week later the government filed a status report with the Court stating that the FBI had successfully obtained access to the data on the Farook iPhone and requesting that the *ex parte* order requiring Apple to assist the FBI be vacated.

Thus, we found that, at the time then-Director Comey testified on February 9 and March 1, the FBI was not in the possession of any means to access the data on the Farook iPhone and believed assistance from Apple would be required to accomplish this. We further found that EAD Hess's April testimony to the effect that rapidly changing technology was a reason that the FBI was not able to exploit the iPhone without assistance was accurate. Accordingly, it does not appear that anyone in OTD withheld knowledge of an FBI capability or that anyone from the FBI testified inaccurately or made false statements at any time regarding same.

IV. Inadequate Communication and Coordination within OTD

The information we obtained during our inquiry suggests that senior managers in OTD were in frequent communication with each other regarding the San Bernardino investigation, including the issues with the Farook iPhone. However, our inquiry also revealed that, in fact, not all relevant personnel had been engaged at the outset.

According to former Assistant Director (AD) of OTD, Stephen Richardson, he had daily conversations with his deputies to receive updates on the efforts to identify a technical solution for the device. AD Richardson described the efforts as a "full court press" to find a solution once it was determined shortly after the attack that they had the suspect's phone, it was locked, and OTD did not have a technique to exploit the device. In addition, we found that briefings provided by AD Richardson and the former Chief of DFAS to their superiors prior to the Congressional testimony and initial court filings accurately reflected their belief at the time that the FBI's capabilities had been researched adequately and that all relevant personnel within OTD had been engaged. We believe FBI leadership relied

on this information as the basis for concluding that the only viable alternative was seeking a court order.

Nevertheless, we were concerned that key personnel were not engaged at the outset of the FBI's efforts. Specifically, on the eve of the February 16 court filing, the ROU Chief had only just begun the process of contacting vendors about a possible technical solution for the Farook iPhone, including contacting an outside vendor who he knew was almost 90 percent finished with a technical solution that would permit the exploitation of the Farook iPhone. Further, we learned that, prior to that time, the CEAU Chief had not verified that ROU had been consulted as part of the outreach to find a technical solution. In addition, we found that the CEAU Chief did not verify or ensure that the question asked during CEAU's outreach efforts was broad enough to elicit responses regarding all possible techniques, not just unclassified ones.

A. According to the ROU Chief, He Was Never Asked to Assist CEAU in its Search for a Solution to the Farook iPhone Problem

According to the ROU Chief, prior to the February 11 managers' meeting, ROU was never asked to assist CEAU in its efforts to find a solution for the Farook iPhone problem, and he was never asked by anyone whether ROU had any current capabilities that might help unlock the phone. In addition, he was certain that the CEAU Chief, specifically, had not reached out to him before or after the February 11 meeting to discuss the phone. According to the ROU Chief, his only conversation with the CEAU Chief was well after the fact, during which the CEAU Chief "was definitely not happy" that the legal proceeding against Apple could no longer go forward.

In the ROU Chief's view, the fact that he was not asked for help sooner was not a mistake in judgment or communication breakdown on CEAU's part, but rather the result of a long-standing policy that the ROU Chief understood created a "line in the sand" against using national security tools in criminal cases. From the time he had become the unit chief in 2010, he was told that ROU's classified techniques could not be used in criminal cases. He said that this dividing line between criminal and national security became part of the culture in OTD and inhibited communication between the criminal and national security components in DFAS and TSS.[3]

[3] The ROU Chief said that the dividing line against using national security techniques in criminal cases originated from a Department policy requiring the approval of the Deputy Attorney General to use such techniques in criminal cases. We believe he was referring to a policy announced in January 2002 by then-Deputy Attorney General Larry Thompson setting forth procedural requirements, including the approval of the Deputy Attorney General, before using classified investigative technologies in criminal cases. *See* Larry D. Thompson, Deputy Attorney General, memorandum to the Assistant Attorney General of the Criminal Division, et al., Procedures for the Use of Classified Investigative Technologies in Criminal Cases, January 31, 2002. The ROU Chief was aware of two instances in which the FBI invoked these procedures, which demonstrated to him that using a classified technique in a criminal case was difficult.

The ROU Chief said that it was this "line in the sand" that led ROU to have no involvement with the Farook iPhone, even after he heard about Comey's testimony on February 9. He said that this all changed 2 days later when the DFAS Chief stated in the February 11 meeting, "If anyone has any kind of solution . . . please let me know." The ROU Chief said that it was the references to "anyone" and "any kind of solution" that prompted him to reach out to his vendors for help, on his own volition. He said he was not asked to do so, and he did not let anyone know he was doing it.

The ROU Chief said that, although possible, he had no recollection of anyone mentioning the Farook iPhone to him before he heard about then-Director Comey's February 9 testimony. The ROU Chief's supervisor, the Chief of TSS, gave us conflicting testimony on this point. The TSS Chief told us during his initial interview that although he was made aware of the Farook iPhone problem at the outset of the investigation, he did not believe it was in his "lane" and did not discuss it with the ROU Chief at that time. In addition, he said he did not task the ROU Chief to help out with the problem until approximately a month before the ROU vendor came forward with a solution (which would place the tasking in mid-February, around or after the time of Comey's testimony, the February 11 managers' meeting, and the USAO's February 16 court filing). According to the TSS Chief, at that time, his supervisors asked him to check with ROU and another unit in his section to see if they had any capabilities that CEAU could use or build upon to exploit the Farook iPhone and, if not, to check with their trusted vendors to see if a vendor could develop a capability. He said that he did not remember receiving an inquiry about ROU's capabilities before this tasking, explaining that "at the onset, [the Farook iPhone] was being handled exclusively by DFAS because that is their mandate" but, later on, his supervisors "tried to pull out all stops and [asked] does anybody have the capability?"

However, after reviewing a draft of this report, the TSS Chief clarified that he believes he did discuss the Farook iPhone with his unit chiefs at the outset of the investigation – for their situational awareness and to see if his units had any current techniques that could assist CEAU. He told the OIG that this discussion would have been followed by a later discussion, sometime after the February 11 meeting (which he did not attend), during which he passed an instruction from his supervisors onto his unit chiefs to have them check with their vendors to see if a vendor could develop a solution. The TSS Chief produced a handwritten note dated December 14, 2015 that he said helped to refresh his recollection on these points. We did not find the note determinative one way or the other on whether the TSS Chief discussed the Farook iPhone with the ROU Chief or asked about ROU's capabilities at the outset of the investigation.[4] Regardless, even under the TSS

[4] Under the heading "Section Chief meetings," the note stated, "√4. Two iPhones from SB shooting → [outside agency]." Based on this note, the TSS Chief believes that he was informed during a routine section chief meeting on December 14, 2015 that DFAS could not access the data on two phones obtained during the investigation and were requesting assistance from another agency. He does not specifically remember, but he infers from this note that he passed this information onto his unit chiefs at his own routine meeting later that day and asked them whether they had "anything in our toolbox that can assist." The TSS Chief said he did not remember whether the ROU Chief

Chief's revised testimony, he and the ROU Chief were never asked or prompted to contact their trusted vendors to see if they could develop a solution until mid-February.

B. The Engagement of ROU Was Not Verified by the CEAU Chief

The CEAU Chief recalled the statement the DFAS Chief made during the February 11 manager's meeting, but he said the meeting would not have been the first time CEAU contacted ROU about the Farook iPhone. According to him, ROU would have been included in CEAU's outreach to see if ROU had a capability in house before this meeting and that the DFAS Chief's statement to the managers at the February 11 meeting was only a final "mop-up" before the application for a court order was filed, just to make sure there was nothing "hiding over here in some other unit" that they did not find.

However, the CEAU Chief was unable to state for certain that ROU had been consulted, who specifically within ROU had been consulted, or whether that person would have been in a position to know the capabilities of the entire unit. According to the CEAU Chief, the search for technical solutions to the Farook iPhone problem was conducted informally by one of CEAU's senior engineers, and informal discussions between the senior engineer and internal FBI components and other agencies were not documented. Further, the CEAU Chief did not ask the senior engineer to identify everyone he contacted as part of the outreach, and he does not remember specifically asking him about ROU. The CEAU Chief only asked the senior engineer whether he had checked with "everybody," and the senior engineer said he had.[5]

According to the CEAU Chief, the senior engineer had many peer relationships, knew what others would have in terms of technical products, and did not need to be told who to contact. The CEAU Chief had faith in the senior engineer's judgment and deferred to him on all technical issues. He told us that he would be "stunned" if it were the case that the senior engineer had not contacted someone in ROU. In contrast to the ROU Chief, the CEAU Chief did not see a line in the sand or wall separating the criminal and national security components in OTD, only a preference not to use classified techniques in criminal cases.[6]

---

attended this later meeting. The ROU Chief told us he did not recall being present during any meeting in which the TSS Chief had this discussion with his unit chiefs.

[5] The CEAU Chief did not recall any data calls or requests from his supervisors to report each of the OTD units CEAU consulted or any conversations with the DFAS Supervisor regarding ROU specifically.

[6] According to the CEAU and ROU Chiefs, it was not often that ROU would be called upon to assist CEAU in a criminal case. Neither the CEAU Chief nor the ROU Chief recalled a specific instance before the Farook iPhone in which ROU provided a technique to assist one of CEAU's criminal cases. Further, the CEAU Chief downplayed the significance of ROU with respect to the Farook iPhone, stating that he did not think ROU conducted a lot of the research and purchasing from vendors that would have been relevant to the efforts to exploit the phone. He said he "was more suspicious . . . not suspicious, I was more thinking that [another unit in OTD] would be the one to come up with something" because the problem was more in [that unit's] purview. He was "a little bit surprised

Regardless of what informal discussions may have occurred at the engineer level, it appears that no one in CEAU consulted the ROU Chief, a step that we believe should have been taken before making any conclusions about ROU's capabilities or the larger question about whether compelling Apple to provide technical assistance was truly necessary. Equally important, we believe the CEAU Chief should have determined all the people and agencies the senior engineer consulted before he and the senior engineer reported to senior OTD management and the USAO that no one could get into the device and that only Apple could provide a technical solution.

C. Question CEAU Asked During Research of Possible Solutions May Not Have Elicited Complete Information

In addition, we found that the CEAU Chief did not verify or ensure that the question asked during CEAU's outreach efforts was broad enough to elicit responses regarding all possible techniques, not just unclassified ones. The CEAU Chief said he believed that the senior engineer would have asked his contacts whether they had any technique that could get into the device, unclassified or otherwise. However, when we asked the CEAU Chief to state the specific question that was posed, he said, "We expect the device, once unlocked, to lead to information which, in all likelihood, if it's inculpatory, would be used in a criminal proceeding. Can [you] help us?" He said the senior engineer would have communicated that the matter was criminal and that the USAO and case agent would want to "pursue a criminal investigation with anything that comes out of the device." He did not know whether the answers they received from internal or external partners were limited to techniques that could be disclosed in court, a point we believe should have been confirmed.[7]

We believe that the emphasis on the fact that the technique would be used to assist a criminal matter could have reasonably and foreseeably led internal and external partners to limit the answers they provided to unclassified techniques only, which, if true, would have created a missed opportunity to explore all possible techniques to unlock the phone. This is troubling regardless of whether a classified technique existed at the time to resolve the FBI's problem.

D. EAD Hess's Concerns and Questions Regarding Whether CEAU Pursued All Possible Avenues

During her OIG interview, EAD Hess told us that at some point during CEAU's efforts to search for a solution, she became concerned that she was not getting a straight answer to the question whether OTD had any way of getting into the phone. She explained to us that OTD is a very large division, and, as it grew, its

---

when ROU was the one who found [the solution]." However, AD Richardson told us that there were at least two avenues available "each and every time" OTD needed to exploit data on a cold, encrypted device – the first was CEAU and the second was ROU.

[7] The DFAS Chief and AD Richardson told us that OTD sought to identify all possible solutions to unlock the Farook iPhone, not just unclassified ones. Further, the DFAS Chief did not believe CEAU had used language focusing only on criminal solutions.

sections and units grew out as individual trees or stovepipes without much integration. She said it always concerned her that individual units do not always know all the capabilities other units have, and that the units are so big that unit chiefs may not even know the full capabilities of their own units. Further, she said that sometimes assumptions are made that "if there was another solution out there, I would know," or sometimes questions are asked, but they are not directed to the right people. Regarding the Farook iPhone specifically, EAD Hess said that although she could not remember when, she remembered a conversation she had with one of OTD's deputy assistant directors who advised her that DFAS did not have a solution for the Farook iPhone. According to Hess, she responded, "That's not what I asked. I asked, does *OTD* know of a solution, have a solution?" and instructed the deputy to ask "everyone else." Inquiries made by EAD Hess may have helped prompt the "mop-up" on February 11.

After the outside vendor successfully demonstrated its technique to the FBI in late March, EAD Hess learned of an alleged disagreement between the CEAU and ROU Chiefs over the use of this technique to exploit the Farook iPhone – the ROU Chief wanted to use capabilities available to national security programs, and the CEAU Chief did not. She became concerned that the CEAU Chief did not seem to want to find a technical solution, and that perhaps he knew of a solution but remained silent in order to pursue his own agenda of obtaining a favorable court ruling against Apple. According to EAD Hess, the problem with the Farook iPhone encryption was the "poster child" case for the Going Dark challenge.[8]

As described earlier, our inquiry did not reveal that anyone in OTD had withheld knowledge of an existing FBI capability, as EAD Hess had feared. However, our inquiry suggests that CEAU did not pursue all possible avenues in the search for a solution. The CEAU Chief told the OIG that, after the outside vendor came forward, he became frustrated that the case against Apple could no longer go forward, and he vented his frustration to the ROU Chief. He acknowledged that during this conversation between the two, he expressed disappointment that the ROU Chief had engaged an outside vendor to assist with the Farook iPhone, asking the ROU Chief, "Why did you do that for?" According to the CEAU Chief, his unit did not ask CEAU's partners to check with their outside vendors. CEAU was only interested in knowing what their partners had in hand – indicating that checking with "everybody" did not include OTD's trusted vendors, at least in the CEAU Chief's mind.[9] However, we believe CEAU should have checked with OTD's trusted vendors for possible solutions before advising OTD management, FBI leadership, or the USAO that there was no other technical alternative and that compelling Apple's assistance was necessary to search the Farook iPhone.

[8] "Going Dark," is often used to describe the eroding ability of law enforcement to use lawful investigative tools to obtain evidence because of changes in technology, such as in the encryption of electronic information. *See* https://www.fbi.gov/services/operational-technology/going-dark (accessed July 20, 2017).

[9] This conflicts with the understanding of the DFAS Chief, who told us he assumed that all relevant OTD units would have contacted their vendors to help find a technique.

V. Conclusions

The OIG found no evidence that OTD had the capability to exploit the Farook iPhone at the time of then-Director Comey's Congressional testimony and the Department's initial court filings. We therefore determined that neither the Congressional testimony nor the submissions to the Court were inaccurate when made. However, FBI statements in Congressional testimony and to the USAO regarding its capabilities to access the data on the Farook iPhone were based on understandings and assumptions that people and units in OTD were effectively communicating and coordinating from the outset and that CEAU had searched for all possible technical solutions, points that were not borne out by the facts, as we determined them.

We received conflicting testimony regarding whether ROU was part of the early outreach efforts to find a solution to the Farook iPhone problem, and we learned that, unbeknownst to anyone, the ROU Chief had only just begun the process of looking for a possible solution to the problem on the eve of the application for a court order being filed – a filing predicated in material part on the notion that technical assistance from Apple was necessary to search the contents of the device. Further, we obtained other information suggesting that not everyone within OTD was on the same page in the search for a technical solution to the Farook iPhone problem, including varying testimony from OTD managers on whether there was a dividing line discouraging collaboration between the units that predominately do criminal and national security work in OTD, the question asked of internal and external partners during CEAU's outreach, whether vendors should have been part of CEAU's outreach effort, and the significance of ROU and the [redacted] on issues relevant to the Farook iPhone problem.[10] Further, the CEAU Chief may not have been interested in researching all possible solutions and instead focused only on unclassified techniques that could readily be disclosed in court and that OTD and its partner agencies already had in-hand. We believe all of these disconnects resulted in a delay in seeking and obtaining vendor assistance that ultimately proved fruitful, and that as a result of the belatedly-obtained technical solution, the government was required to withdraw from its previously stated position that it could not access the

[10] [redacted] to address the "Going Dark" problem, including the encryption issues with current iPhone devices. According to the TSS Chief's handwritten notes, he attended a [redacted] steering committee meeting in mid-December during which the topic of defeating PIN encryption was discussed. He did not recall the meeting or who attended, but he said the timing of the discussion was likely prompted by the Farook iPhone problem. Further, the DFAS Chief told us that he asked CEAU to make sure it consulted [redacted] regarding the Farook iPhone and learned from the CEAU Chief that [redacted] did not have anything that could unlock the phone. The DFAS Chief said that he also recalled going [redacted] himself in mid-January 2016 to get a status update on [redacted] efforts to find solutions for the new iPhone operating systems. By contrast, the CEAU Chief down-played the significance of [redacted] with respect to the Farook iPhone, stating that [redacted] did not focus its research on the capabilities and exploits that would have been helpful. He said it was possible CEAU consulted [redacted], but he did not remember [redacted] being involved at all with the San Bernardino investigation.

iPhone in this critical case, and by implication in other cases, without first compelling cooperation from the manufacturer.

After reviewing a draft of this report, the FBI represented to the OIG that there was no delay in the ROU vendor's development of the technique that ultimately allowed the FBI to exploit the Farook iPhone. According to the FBI, the vendor "indicated that they had been working on this solution as part of a larger project for some time, as this was a well-known investigative need for numerous law enforcement and national security agencies throughout the world." Further, after reviewing the draft report, the FBI told us that during a meeting in November 2017 on unrelated matters, a representative of the outside vendor indicated that the vendor had developed the technique that provided access to the Farook iPhone on its own and proactively notified the FBI. The FBI did not describe the purpose of this meeting or who participated in the meeting on behalf of the FBI and, more importantly, on behalf of the vendor.

The suggestion that the outside vendor had developed the technique by March 16, without any request to prioritize the matter or communication from the ROU Chief, is not consistent with the testimony of the ROU Chief who told us unequivocally that he had requested the vendor's assistance the month before. The ROU Chief, who described himself as the "relationship holder" for this particular vendor at the time of the San Bernardino investigation, told us that this vendor was not actively working on this particular solution when he contacted the vendor in mid-February 2016. According to the ROU Chief, this vendor had multiple priorities and was working on many projects, changing focus between projects as priorities shifted. Before being contacted by the ROU Chief, the vendor had completed almost 90 percent of what was needed to gain access to devices of the same model and operating system as the Farook iPhone, but it was not actively working on the remaining 10 percent. The ROU Chief said that in response to his request for assistance, the vendor reallocated its resources to finish the remaining 10 percent, moving this particular solution to the "front burner."

The ROU Chief's testimony is consistent with the testimony of his supervisor, the TSS Chief, that the ROU Chief had asked this vendor for assistance a month before the vendor came forward with the solution, as well as the testimony of the CEAU Chief that he had expressed frustration that the ROU Chief had accelerated the development of a technical solution before the conclusion of the legal proceeding against Apple. However, regardless of whether the FBI agrees that the ROU Chief acted as a catalyst in mid-February, the fact remains that the ROU Chief knew, as the relationship holder, that this particular vendor had completed almost 90 percent of what was necessary to gain access to the Farook iPhone – knowledge that we believe should have been made known to FBI leadership and the USAO early in the San Bernardino investigation so that they could have considered that information in deciding whether and when to pursue legal action against Apple. We believe better communication and coordination at the outset among the units in OTD would have helped to ensure that this had taken place.

VI. Recommendation to Improve Communication and Coordination

At the time of the San Bernardino investigation, OTD did not have written protocol or formal guidance governing the steps that should be taken to de-conflict technical capabilities within OTD or the due diligence necessary regarding same before filing an affidavit in court attesting to FBI's capabilities. After the government withdrew the court filing against Apple, senior OTD management told CEAU that it must de-conflict with ROU, as well as certain other units, whenever addressing devices in need of a technical solution.

The FBI told us that it is taking further steps to address the circumstances that contributed to this incident. During the course of our inquiry, we were informed that the FBI intends to add a new section in OTD to consolidate resources to address the "Going Dark" problem and improve coordination between the units that work on computer and mobile devices. We believe that such efforts to improve communication and coordination are worthwhile, and should help to avoid some of the disconnects we found occurred in this very important and high profile investigation.

Accordingly, we recommend that the FBI take the necessary steps to finalize the reorganization and any other actions appropriate to ensure the full coordination that such incidents clearly demand. Please provide us with a status report on the FBI's implementation of this recommendation within 90 days.

APPENDIX A

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 9, 2018

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation.*

We are pleased that you found, "...that neither the Congressional testimony nor the submissions to the Court were inaccurate when made."

We agree that it is important to take steps to improve communication and coordination through a reorganization within the Operational Technology Division. In that regard, we concur with your recommendation for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

Thomas G. Seiler
Acting Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation

FBI's Response to the OIG Recommendation
March 9, 2018

Recommendation: Recommend that the FBI take the necessary steps to finalize the reorganization and any other actions appropriate to ensure the full coordination that such incidents clearly demand.

FBI Response to OIG Recommendation:

The problems noted in the OIG report were due to communication issues between the FBI/OTD Unit Chiefs; these problems were addressed through a change in leadership for the Units involved. Also, FBI/OTD has realigned mission areas for several Units in preparation for a larger re-organization.

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.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL
950 Pennsylvania Avenue, Northwest
Suite 4760
Washington, DC 20530-0001

Website	**Twitter**	**YouTube**
oig.justice.gov	@JusticeOIG	JusticeOIG

Also at Oversight.gov