

**Congress of the United States**  
**Washington, DC 20515**

April 13, 2018

The Honorable Christopher Wray  
Federal Bureau of Investigations  
935 Pennsylvania Avenue, NW  
Washington, DC 20535

Dear Director Wray,

Recently, the Department of Justice's Office of Inspector General (OIG) released a troubling report on the Bureau's handling of Syed Rizwan Farook's iPhone in the aftermath of the San Bernardino attack. The OIG report finds that the primary forensics unit responsible for unlocking the iPhone did not consult with third-party vendors, nor did it consult with relevant FBI offices, including the Remote Operations Unit (ROU) which already knew of a potential solution.

Perhaps most disturbingly, statements made by the Chief of the Cryptographic and Electronic Analysis Unit appear to indicate that the FBI was more interested in forcing Apple to comply than getting into the device.

The OIG report finds that the FBI's lead forensics team working Farook's iPhone, the Cryptographic and Electronic Analysis Unit (CEAU) did not consult with other FBI experts, such as the ROU or third-party vendors, to determine what capabilities or relationships could be leveraged to unlock the phone. The report concludes that the "CEAU should have checked with OTD's trusted vendors for possible solutions before... compelling Apple's assistance..."<sup>1</sup> and that "no one in CEAU consulted the ROU Chief, a step that we believe should have been taken before making any conclusions about... whether compelling Apple to provide technical assistance was truly necessary."<sup>2</sup>

It was not until the night before FBI's suit against Apple, which was predicted "on the notion that technical assistance from Apple was necessary to search the contents of the device,"<sup>3</sup> that the FBI first consulted the third-party vendor that it knew had nearly completed a solution.

But even more concerning is the OIG's find that the ROU Chief reached out to the vendor on his own volition and was chastised by the CEAU Chief for doing so:

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

---

<sup>1</sup> Office of Inspector General, Department of Justice, Report: *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*, page 8

<sup>2</sup> *Id.* page 6

<sup>3</sup> *Id.* page 9

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?”<sup>4</sup>

The report also finds that the FBI’s former Executive Assistant Director for Science and Technology, Amy Hess, was concerned that FBI agents were not exhausting all technical options precisely because they wanted the suit against Apple to go forward:

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.**<sup>5</sup>

This report undermines statements that the FBI made during the San Bernardino litigation and consistently since then, that only the device manufacturer could provide a solution. Moreover, recent reports that companies such as Cellebrite<sup>6</sup> and GrayShift<sup>7</sup> have developed tools to cheaply unlock nearly every phone on the market, including every version of iOS, raise even more concerns that the FBI has not been forthcoming about the extent of the “Going Dark” problem. The service offered by Cellebrite, the company alleged to have unlocked Farook’s iPhone, reportedly costs about \$1500 per phone to unlock. The second company, Greyshift, reportedly offers a device that was recently purchased by the State Department that will unlock phones at a cost of about \$50 per phone.

According to your testimony and public statements, the FBI encountered 7,800 devices last year that it could not access due to encryption. However, in light of the availability of unlocking tools developed by third-parties and the OIG report’s findings that the Bureau was uninterested in seeking available third-party options, these statistics appear highly questionable.

Please provide answers to the following questions as soon as possible:

- Have you consulted with relevant third-party vendors to understand what tools are available to help the FBI access device content?
- Do you agree that there are solutions available to help unlock or decrypt nearly every device on the market? If not, why are these solutions, particularly the ones discussed above, insufficient?
- Why can’t the FBI unlock the 7,800 devices? Have you attempted to use tools developed by third-parties to unlock these devices?

---

<sup>4</sup> *Id.* page 8

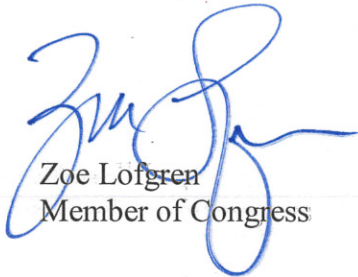
<sup>5</sup> *Id.* page 1 (emphasis added)

<sup>6</sup> <https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#5f03bdb4667a>


<sup>7</sup> [https://motherboard.vice.com/en\\_us/article/kzxwwz/state-department-seemingly-buys-dollar15000-iphone-cracking-tech-graykey](https://motherboard.vice.com/en_us/article/kzxwwz/state-department-seemingly-buys-dollar15000-iphone-cracking-tech-graykey)

- Of these locked phones, how many are equipped with biometrics or how many have data available through a cloud service, which would provide additional means to access data or unlock phones?
- For each device that you have not used a third-party tool to unlock, what is the rationale for not doing so?

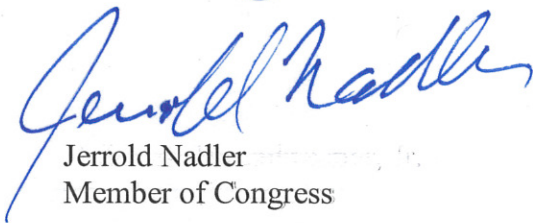
Sincerely,




Zoe Lofgren  
Member of Congress




Darrell Issa  
Member of Congress



Jerrold Nadler  
Member of Congress



F. James Sensenbrenner, Jr.  
Member of Congress



Ted W. Lieu  
Member of Congress



Ted Poe  
Member of Congress



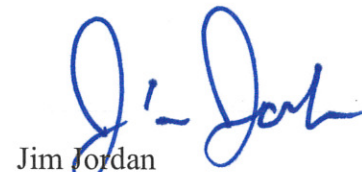
Jared Polis  
Member of Congress



Matt Gaetz  
Member of Congress



Suzan DelBene  
Member of Congress



Jim Jordan  
Member of Congress