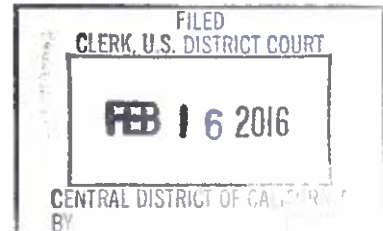FILED
COPY
2016 FEB 16 AM 11: 00
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
BY_____

1  EILEEN M. DECKER
   United States Attorney
2  PATRICIA A. DONAHUE
   Assistant United States Attorney
3  Chief, National Security Division
   TRACY L. WILKISON (California Bar No. 184948)
4  Assistant United States Attorney
   Chief, Cyber and Intellectual Property Crimes Section
5  ALLEN W. CHIU (California Bar No. 240516)
   Assistant United States Attorney
6  Terrorism and Export Crimes Section
        1500 United States Courthouse
7       312 North Spring Street
        Los Angeles, California 90012
8       Telephone:  (213) 894-0622/2435
        Facsimile:  (213) 894-8601
9       Email:      Tracy.Wilkison@usdoj.gov
                    Allen.Chiu@usdoj.gov
10
   Attorneys for Applicant
11 UNITED STATES OF AMERICA

12              UNITED STATES DISTRICT COURT

13          FOR THE CENTRAL DISTRICT OF CALIFORNIA

14 IN THE MATTER OF THE SEARCH OF      ED No. 15-0451M
   AN APPLE IPHONE SEIZED DURING
15 THE EXECUTION OF A SEARCH           GOVERNMENT'S *EX PARTE* APPLICATION
   WARRANT ON A BLACK LEXUS IS300,     FOR ORDER COMPELLING APPLE INC. TO
16 CALIFORNIA LICENSE PLATE            ASSIST AGENTS IN SEARCH;
   35KGD203                            MEMORANDUM OF POINTS AND
17                                     AUTHORITIES; DECLARATION OF
                                       CHRISTOPHER PLUHAR; EXHIBIT
18

19

20       The United States of America, by and through its counsel,

21 Assistant United States Attorneys Tracy L. Wilkison and Allen W.

22 Chiu, hereby applies to the Court ex parte pursuant to the All Writs

23 Act, 28 U.S.C. § 1651, for an order that Apple Inc. ("Apple") provide

24 assistance to agents of the Federal Bureau of Investigation ("FBI")

25 in their search of a cellular telephone, Apple make: iPhone 5C,

26 Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI:

27 358820052301412, on the Verizon Network (the "SUBJECT DEVICE").  The

28 search and seizure of the SUBJECT DEVICE was authorized through a

1 | search warrant which was obtained on December 3, 2015, Docket Number
2 | ED No. 15-0451M, and was executed on the same day.
3 | This application is based on the attached declaration of FBI
4 | Supervisory Special Agent Christopher Pluhar, and the files and
5 | records of this case, including the underlying search warrant, which
6 | is attached hereto as Exhibit 1.
7 | Dated: February 16, 2016          Respectfully submitted,

8 | EILEEN M. DECKER
United States Attorney
9 |
PATRICIA A. DONAHUE
10 | Assistant United States Attorney
Chief, National Security Division
11 |

12 |

13 | TRACY L. WILKISON
ALLEN W. CHIU
14 | Assistant United States Attorneys

15 | Attorneys for Applicant
UNITED STATES OF AMERICA
16 |

## MEMORANDUM OF POINTS AND AUTHORITIES

### I. INTRODUCTION

In the hopes of gaining crucial evidence about the December 2, 2015 massacre in San Bernardino, California, the government has sought to search a lawfully-seized Apple iPhone used by one of the mass murderers. Despite both a warrant authorizing the search and the phone owner's consent, the government has been unable to complete the search because it cannot access the iPhone's encrypted content. Apple has the exclusive technical means which would assist the government in completing its search, but has declined to provide that assistance voluntarily. Accordingly, the government respectfully requests that this Court issue an order compelling Apple to assist in enabling the search commanded by the warrant.

### II. FACTUAL BACKGROUND

The Federal Bureau of Investigation ("FBI") is in possession of a cellular telephone that was used by Syed Rizwan Farook ("Farook"), one of the terrorists who caused the December 2, 2015 shooting death of 14 people, and the shooting and injuring of 22 others, at the Inland Regional Center ("IRC") in San Bernardino, California. The cellular telephone is of Apple make: iPhone 5C, Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, on the Verizon Network ("the SUBJECT DEVICE"). The SUBJECT DEVICE was seized pursuant to a federal search warrant for a black Lexus IS300 in Docket Number ED 15-0451M, which was issued by the Honorable David T. Bristow, United States Magistrate Judge, on December 3, 2015. The underlying search warrant, which authorizes the search of the contents of the SUBJECT DEVICE, is attached hereto as Exhibit 1 and incorporated herein by reference.

As explained in the attached declaration of FBI Supervisory Special Agent ("SSA") Christopher Pluhar, the underlying search warrant for the SUBJECT DEVICE arose out of an investigation into the IRC shootings, and the participation by Farook and his wife, Tafsheen Malik ("Malik"), in that crime. Subsequent to execution of the search warrant at issue, the FBI obtained numerous search warrants to search the digital devices and online accounts of Farook and Malik. Through those searches, the FBI has discovered, for example, that on December 2, 2015, at approximately 11:14 a.m., a post on a Facebook page associated with Malik stated, "We pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi," referring to Abu Bakr Al Baghdadi, the leader of Islamic State of Iraq and the Levant ("ISIL"), also referred to as the Islamic State ("IS"), the Islamic State of Iraq and al-sham ("ISIS"), or Daesh. ISIL, formerly known as Al-Qai'da in Iraq ("AQI"), has been designated a foreign terrorist organization by the United States Department of State, and has been so designated since December 2004. Farook and Malik died later that same day in a shoot-out with law enforcement. The government requires Apple's assistance to access the SUBJECT DEVICE to determine, among other things, who Farook and Malik may have communicated with to plan and carry out the IRC shootings, where Farook and Malik may have traveled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement in the deadly shooting.

The SUBJECT DEVICE is owned by Farook's employer, the San Bernardino County Department of Public Health ("SBCDPH"), and was assigned to, and used by, Farook as part of his employment. The

SBCDPH has given its consent to the search of the SUBJECT DEVICE and to Apple's assistance with that search.[1]

However, despite the search warrant and the owner's consent, the FBI has been unable to search the SUBJECT DEVICE because it is "locked" or secured with a user-determined, numeric passcode. More to the point, the FBI has been unable to make attempts to determine the passcode because Apple has written, or "coded," its operating systems with a user-enabled "auto-erase function" that would, if enabled, result in the permanent destruction of the required encryption key material after 10 erroneous attempts at the passcode (meaning that after 10 failed attempts at inputting the passcode, the information on the device becomes permanently inaccessible). When an Apple iPhone is locked, it is not apparent from the outside whether or not that auto-erase function is enabled; therefore, trying repeated passcodes risks permanently denying all access to the contents. Primarily because of this function and the delays that would be introduced by successive incorrect passcodes (discussed below), the government has not been able to attempt to determine the passcode and decrypt the files on the SUBJECT DEVICE pursuant to the search warrant, and the FBI cannot do so without Apple's assistance.

Apple is the manufacturer of the SUBJECT DEVICE, and the creator and owner of its operating system and software. Apple has the ability with older operating systems to obtain the unencrypted file content from phones without the passcode, and has routinely done so for law enforcement with a search warrant and accompanying

_____

[1] In addition, SBCDPH has a written policy that all digital devices are subject to search at any time by the SBCDPH, which policy Farook accepted via signature upon his employment.

3

All Writs Act order.  While Apple has publicized that it has written the software differently with respect to iPhones such as the SUBJECT DEVICE with operating system ("iOS") 9, Apple yet retains the capacity to provide the assistance sought herein that may enable the government to access the SUBJECT DEVICE pursuant to the search warrant.

Specifically, and as detailed below, Apple has the ability to modify software that is created to only function within the SUBJECT DEVICE that would ensure that the added auto-erase function is turned off, allow for electronic submission of test passcodes, and ensure additional delays are not created.  This would allow the government multiple investigative attempts to determine the passcode in a timely manner, without fear that the data subject to search under the warrant would be rendered permanently inaccessible.  It is this assistance from Apple, which is required to execute the search warrant, that the government now asks the Court to order.

III. DISCUSSION

A.    Assistance Sought From Apple

In sum, the government seeks an order that Apple assist in enabling the search commanded by the warrant by removing, for the SUBJECT DEVICE only, some of the additional, non-encryption barriers that Apple has coded into its operating system, such as the auto-erase function, the requirement that passwords be entered manually, and any software-invoked delay-upon-failure functions.  While the government proposes a specific means of accomplishing this, the government requests that the order allow Apple to achieve the goals of the order in an alternative technical manner if mutually preferable.

4

As an initial matter, the assistance sought can only be provided by Apple. As discussed in the attached declaration of SSA Pluhar, the SUBJECT DEVICE is an iPhone 5c that was designed, manufactured, and sold by Apple. Apple also wrote and owns the software operating system marketed under the name of "iOS," and thus is the owner of the operating system software for the phone at issue. Apple's software licensing agreement specifies that its software is "licensed, not sold," and otherwise prohibits users from transferring any ownership of the iOS software.

Further to this point, Apple strictly and exclusively controls the hardware and software that is used to turn on and run its phones. According to Apple's "white papers" and other publicly available information about the security of its iOS programs, Apple has designed its mobile device hardware, as well as its operating system software, to only permit and run software that has been "signed" cryptographically by Apple using its own proprietary encryption methods. These security features prevent other persons, including the government, from running any other software on the SUBJECT DEVICE to attempt to recover data or test passcodes.

Apple has designed the iOS 9 operating system for its phones to encrypt the data files by a combination of two components – one user-determined passcode, and one unique 256-bit Advanced Encryption Standard ("AES") key (referred to as a "UID") which is fused into the phone itself during manufacture. Both passcode components are required in combination for the operating system to decrypt the phone's data files. When a user inputs her passcode, the phone conducts a complex calculation as determined by Apple's software

5

(and unknown to the government) which combines the UID with the user passcode. If the result is accurate, the data is decrypted.

If one does not know the user-determined passcode, it is possible, although time-consuming, to manually input passcodes one at a time until the passcode is determined. Apple, however, has also designed and written code for additional non-encryption-based features which the government cannot overcome on its own.

First, Apple has designed a non-encryption, auto-erase function as part of its iOS, which destroys the encryption key materials required for decryption and hence renders the contents of the device permanently incapable of being decrypted after ten consecutive incorrect passcode attempts. If this auto-erase function is enabled, the operating system will instantly, irrecoverably, and without warning erase the encryption keys necessary for accessing stored data. There is no way to know by examining the outside of the phone whether or not this function has been enabled, although, in this instance, the government suspects that it has, for the reasons explained in the attached declaration of SSA Pluhar - including because the SBCDPH has stated that the SUBJECT DEVICE was provided to Farook with that function turned on, and the most recent backup from the iCloud showed the function turned on. Accordingly, trying successive passcodes risks permanently losing the ability to access the data on the SUBJECT DEVICE. Because iOS software must be cryptographically signed by Apple, only Apple is able to modify the iOS software to change the setting or prevent execution of the function.

Relatedly, Apple has designed and written code for another non-encryption-based feature in that its iOS operating system is coded

6

to invoke time delays after repeated, unsuccessful passcode entries. This means that after each failed passcode entry, the user must wait a period of time before another attempt can be made, up to a 1-hour delay after the ninth failed attempt. Additional wait times can also be added into the software.

In order to overcome these hurdles, the government seeks an order requiring Apple to assist in the execution of a search warrant using the capabilities that Apple has retained along within its encryption software, such that the government can attempt to determine the passcode without these additional, non-encryption features that Apple has coded into its operating system, for the SUBJECT DEVICE only. Apple's assistance would permit the government to electronically test passcodes without unnecessary delay or fear that the data subject to search under the warrant would be rendered permanently inaccessible. Given that these features were designed and implemented by Apple, that Apple writes and cryptographically signs the iOS, and that Apple routinely patches or updates its iOS to address security features or other functionality, modifying these features is well within its technical capabilities.

Specifically, in order to perform the search ordered in the warrant, the government requests that Apple be ordered to provide the FBI with a custom signed iPhone Software ("IPSW") file, recovery bundle, or other Software Image File ("SIF")[2] that can be loaded onto the SUBJECT DEVICE. The SIF would load and run from Random Access

---

[2] These are different terms for the essentially same thing: a software file that will start up/"boot" an iPhone device.

7

Memory ("RAM")[3] and accordingly would not change the operating system on the actual SUBJECT DEVICE, the user data partition (i.e., where the contents of files created or modified by the user are stored), or system partition on the device's flash memory. Importantly, the SIF would be created with a unique identifier of the SUBJECT DEVICE so that the SIF would only load and execute on the SUBJECT DEVICE.[4]

Once active on the SUBJECT DEVICE, the SIF would have three primary functions: (1) the SIF would bypass or disable the auto-erase function whether or not it has been enabled; (2) the SIF would enable the FBI to submit passcodes to the SUBJECT DEVICE for testing electronically (meaning that the attempts at the passcode would not have to be manually typed on the iPhone's screen; and (3) the SIF would not introduce any additional delay between failed passcode attempts beyond what is incurred by the hardware on the SUBJECT DEVICE. The SIF would be installed on the SUBJECT DEVICE at either a government facility, or alternatively, at an Apple facility (as is done when Apple recovers data from earlier iOS versions), but passcode attempts would be electronically submitted to the device by the government. This would allow the government to conduct the passcode attempts while Apple retains the SIF. The government further requests that the order permit Apple to satisfy these three

---

[3] RAM is computer memory that is temporary and requires power to maintain the stored information; once the power is turned off, the memory is lost.

[4] Since Apple's software currently has the capability to query hardware for unique identifiers (serial numbers, ECID, IMEI, etc.), the SIF could be created to only function on the SUBJECT DEVICE, which would mitigate any perceived risk to Apple iOS software as to any other Apple device. As an alternative, the government would be willing to test the passcodes remotely while the SUBJECT DEVICE is in Apple's possession.

goals, and installation and operation within the SUBJECT DEVICE, in an alternative technical manner if mutually preferable.

## B.    The All Writs Act Permits This Order

The All Writs Act provides in relevant part that "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."  28 U.S.C. § 1651(a).  As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute."  Pennsylvania Bureau of Correction v. United States Marshals Service, 474 U.S. 34, 43 (1985).  The All Writs Act permits a court, in its "sound judgment," to issue orders necessary "to achieve the rational ends of law" and "the ends of justice entrusted to it."  United States v. New York Telephone Co., 434 U.S. 159, 172-3 (1977) (citations and internal quotation marks omitted).  Courts must apply the All Writs Act "flexibly in conformity with these principles."  Id. at 173; accord United States v. Catoggio, 698 F.3d 64, 67 (2d Cir.2012) ("[C]ourts have significant flexibility in exercising their authority under the Act.") (citation omitted).

Pursuant to the All Writs Act, the Court has the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers."  Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979) (citing United States v. New York. Tel. Co., 434 U.S. 159 (1977)); see also In re U.S. for an Order Directing a Provider of Communication Services to Provide Technical Assistance to Agents of the U.S. Drug Enforcement Administration, 2015 WL 5233551 (D.P.R. August 27, 2015) (granting government's request pursuant to the All Writs Act for

9

technical assistance from provider of electronic communication

services to provide information, facilities, and technical

assistance to facilitate the consensual recording of all electronic

communication to and from a particular mobile phone); United States

v. Fricosu, 841 F.Supp.2d 1232, 1238 (D.Colo. 2012) (order issued

under All Writs Act requiring defendant to provide password to

encrypted computer seized pursuant to a search warrant).  In New

York Telephone Co., the Supreme Court held that courts have

authority under the All Writs Act to issue supplemental orders to

third parties to facilitate the execution of search warrants.  The

Court held that "[t]he power conferred by the Act extends, under

appropriate circumstances, to persons who, though not parties to the

original action or engaged in wrongdoing, are in a position to

frustrate the implementation of a court order or the proper

administration of justice, . . . and encompasses even those who have

not taken any affirmative action to hinder justice."  Id. at 174.

In particular, the Court upheld an order directing a phone company

to assist in executing a pen register search warrant issued under

Rule 41.  See id. at 171-76; see also Application of U.S. for an

Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel.

Facilities (Mountain Bell), 616 F.2d 1122, 1132-33 (9th Cir. 1980)

(affirming district court's order compelling Mountain Bell to trace

telephone calls on grounds that "the obligations imposed . . . were

reasonable ones." (citing New York Tel. Co., 434 U.S. at 172)).

New York Telephone Co. also held that "Rule 41 is not limited

to tangible items but is sufficiently flexible to include within its

scope electronic intrusions authorized by a finding of probable

cause."  434 U.S. at 170.  The Court relied upon the authority of a

search warrant pursuant to Rule 41 to predicate an All Writs Act order commanding a utility to implement a pen register and trap and trace device — before Congress had passed a law that specifically authorized pen registers by court order. Under New York Telephone Co. and Mountain Bell, the All Writs Act provides authority for this Court to order Apple to assist with steps necessary to perform the search ordered by the warrant for the SUBJECT DEVICE.

Further, based on the authority given to the courts under the All Writs Act, courts have issued orders, similar to the one the government is seeking here, that require a manufacturer to assist in accessing a cell phone's files so that a warrant may be executed as originally contemplated. See, e.g., In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014); see also United States v. Navarro, No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013). Courts have also issued All Writs Act orders in furtherance of warrants in a wide variety of contexts, including: ordering a defendant to produce a copy of the unencrypted contents of a computer seized pursuant to a federal search warrant (Fricosu, 841 F.Supp. 2d at 1238); ordering a phone company to assist with a trap and trace device (Mountain Bell, 616 F.2d 1122, 1129 (9th Cir. 1980)); ordering a credit card company to produce customer records (United States v. Hall, 583 F. Supp. 717, 722 (E.D. Va. 1984)); ordering a landlord to provide access to security camera videotapes (In re Application of United States for an Order Directing X to Provide Access to Videotapes, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (unpublished order)); and ordering a phone company to assist with consensual monitoring of

11

a customer's calls (<u>In re U.S.</u>, No. 15-1242 (M), 2015 WL 5233551, at *4-5 (D.P.R. Aug. 27, 2015) (unpublished order)). Because the orders are typically, as here, sought in the midst of a criminal investigation, they are usually obtained by way of <u>ex parte</u> application and not noticed motion. <u>See</u>, <u>e.g.</u>, <u>New York Telephone Co.</u>, 434 U.S. at 162; <u>In re U.S.</u>, 2015 WL 5233551, at *1; <u>In re [XXX]</u>, 2014 WL 5510865, at *1; <u>Application of U.S.</u>, 616 F.2d at 1122; <u>In re Application of United States</u>, 2003 WL 22053105, at *1. The government is not aware of any case in which the government obtained a Rule 41 search warrant but was denied an All Writs Act Order when necessary to facilitate the execution of the warrant.[5]

In <u>New York Telephone Co.</u>, the Supreme Court considered three factors in concluding that the issuance of the All Writs Act order to the phone company was appropriate. First, it found that the phone company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." <u>Id.</u> at 174. Second, it concluded that the order did not place an undue burden on the phone company. <u>See id.</u> at 175. Third, it determined that the assistance of the company was necessary to

---

[5] The government is also aware of multiple other unpublished orders in this district and across the country (obtained by ex parte application) compelling Apple to assist in the execution of a search warrant by accessing the data on devices running earlier versions of iOS, orders with which Apple complied. The only exception known to the government is litigation pending before a Magistrate Judge in the Eastern District of New York, where that court <u>sua sponte</u> raised the issue of whether it had authority under the All Writs Act to issue a similar order. That out-of-district litigation remains pending without any issued orders, nor would any such order be binding on this court. In any event, those proceedings represent a change in Apple's willingness to access iPhones operating prior iOS versions, not a change in Apple's technical ability. However, based on that litigation and communications with Apple, the government anticipates that Apple will avail itself of its ability to apply for relief pursuant to the proposed order.

achieve the purpose of the warrant.  See id.  Each of these factors

supports issuance of the order directed to Apple in this case.

      1.    Apple is not "far removed" from this matter

      First, Apple is not "so far removed from the underlying

controversy that its assistance could not be permissibly compelled."

Apple designed, manufactured and sold the SUBJECT DEVICE, and wrote

and owns the software that runs the phone — which software is

preventing the execution of the warrant.  Indeed, Apple has

positioned itself to be essential to gaining access to the SUBJECT

DEVICE or any other Apple device, and has marketed its products on

this basis.  Apple designed and restricts access to the code for the

auto-erase function — the function that makes the data on the phone

permanently inaccessible after multiple failed passcode attempts and

thus effectively prevents the government from attempting to execute

the search warrant without Apple's assistance.  The same software

Apple is uniquely able to modify also controls the delays Apple

implemented between failed passcode attempts -- which makes the

process take too long to enable the access ordered by the court.

Especially but not only because iPhones will only run software

cryptographically signed by Apple, and because Apple restricts

access to the code of the software that creates these obstacles,

there is no other party that has the ability to assist the

government in preventing these features from obstructing the search

ordered by the court pursuant to the warrant.

      Apple is also not made "far removed" by the fact that it is a

non-government third party.  While New York Telephone Co. involved a

public utility, that was not the source of the holding that the All

Writs Act order was appropriate.  New York Telephone Co. emphasized

13

that "the Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis," and the company's noncompliance "threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used." New York Telephone Co., 434 U.S. at 174. By analogy, where Apple manufactured and sold a phone used by a person at the center of a terrorism investigation, where it owns and licensed the software used to "facilitate the criminal enterprise," where that very software now must be used to enable the search ordered by the warrant, compulsion of Apple is permissible under New York Telephone Co. Moreover, other courts have directed All Writs Act orders based on warrants to entities that are not public utilities. For example, neither the credit card company in Hall nor the landlord in Access to Videotapes was a public utility. See Hall, 583 F. Supp. at 722; Access to Videotapes, 2003 WL 22053105, at *3. Apple's close relationship to the iPhone and its software – which are by Apple's design – makes compelling assistance from Apple permissible and the only means of executing the warrant.

        2.    The order does not place an unreasonable burden on Apple

Second, the order is not likely to place any unreasonable burden on Apple. Where, as here, compliance with the order would not require inordinate effort, and reasonable reimbursement for that effort is available, no unreasonable burden can be found. New York Telephone, 434 U.S. at 175 (holding that All Writs Act order was not burdensome because it required minimal effort by the company, provided for reimbursement for the company's efforts, and did not disrupt its business operations); Mountain Bell, 616 F.2d at 1132

(rejecting telephone company's argument that unreasonable burden would be imposed because of a drain on resources and possibility of system malfunctions because the "Order was extremely narrow in scope, restricting the operation to [electronic switching system] facilities, excluding the use of manual tracing, prohibiting any tracing technique which required active monitoring by company personnel, and requiring that operations be conducted 'with a minimum of interference to the telephone service'").

While the order in this case requires Apple to provide modified software, modifying an operating system – writing software code – is not an unreasonable burden for a company that writes software code as part of its regular business. In fact, providers of electronic communications services and remote computing services are sometimes required to write code in order to gather information in response to subpoenas or other process. In addition, the order is tailored for this particular phone, and because it involves preparing a single SIF, it presents no danger of system malfunctions or disrupting business operations. As noted above, Apple designs and implements all of the features discussed, writes and cryptographically signs the iOS, and routinely patches security or functionality issues in its operating system and releases new versions of its operating system to address issues. By comparison, writing a program that turns off non-encryption features that Apple was responsible for writing to begin with would not be unduly burdensome.[6]

---

[6] It is worth noting as well that the user of the phone is now dead, the user was made aware of his lack of privacy in the work phone while alive, and the owner of the phone consents to both the search of the phone and to Apple's assistance in this matter.

However, to the extent that Apple believes that compliance with the order would be unreasonably burdensome, it can make an application to the Court for relief prior to being compelled to provide the assistance. See In re XXX, 2014 WL 5510865, at *2 (including in the issued All Writs Act Order a provision that states that "to the extent [the manufacturer] believes that compliance with this Order would be unreasonably burdensome, it may delay compliance provided it makes an application to the Court for relief within five business days of receipt of the Order."). The proposed order in this case includes a similar directive.

       3.    Apple's assistance is necessary to effectuate the warrant

Third, Apple's assistance is necessary to effectuate the warrant. In New York Telephone Co., the Court held that the order met that standard because "[t]he provision of a leased line by the Company was essential to the fulfillment of the purpose — to learn the identities of those connected with the gambling operation — for which the pen register order had been issued." 434 U.S. at 175. Here, the proposed All Writs Act order in this matter also meets this standard, as it is essential to ensuring that the government is able to perform the search ordered by the warrant.

In this case, the ability to perform the search ordered by the warrant on the SUBJECT DEVICE is of particular importance. The user of the phone, Farook, is believed to have caused the mass murder of a large number of his coworkers and the shooting of many others, and to have built bombs and hoarded weapons for this purpose. The government has been able to obtain several iCloud backups for the SUBJECT DEVICE, and executed a warrant to obtain all saved iCloud

16

data associated with the SUBJECT DEVICE. Evidence in the iCloud account indicates that Farook was in communication with victims who were later killed during the shootings perpetrated by Farook on December 2, 2015, and toll records show that Farook communicated with Malik using the SUBJECT DEVICE. Importantly, however, the most recent backup of the iCloud data obtained by the government was dated October 19, 2015, approximately one-and-a-half months before the shooting. This indicates to the FBI that Farook may have disabled the automatic iCloud backup function to hide evidence, and demonstrates that there may be relevant, critical communications and data around the time of the shooting that has thus far not been accessed, may reside solely on the SUBJECT DEVICE, and cannot be accessed by any other means known to either the government or Apple.

As noted above, assistance under the All Writs Act has been compelled to provide decrypted contents of devices seized pursuant to a search warrant. In Fricosu, a defendant's computer — whose contents were encrypted — was seized, and defendant was ordered pursuant to the All Writs Act to assist the government in producing a copy of the unencrypted contents of the computer. 841 F.Supp. 2d at 1237 ("There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production."). Here, the type of assistance does not even require Apple to assist in producing the unencrypted contents, the assistance is rather to facilitate the FBI's attempts to test passcodes.

# IV. CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court order Apple to assist the FBI in the search of the SUBJECT DEVICE as detailed in the proposed order.

Dated: February 16, 2016          Respectfully submitted,

EILEEN M. DECKER
United States Attorney

PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division

*Tracy Wilke*

TRACY L. WILKISON
ALLEN W. CHIU
Assistant United States Attorneys

Attorneys for Applicant
UNITED STATES OF AMERICA

# DECLARATION OF CHRISTOPHER PLUHAR

I, Christopher Pluhar, being duly sworn, declare and state as follows:

## I.  INTRODUCTION

1.   I am a Supervisory Special Agent ("SSA") with the Federal Bureau of Investigation ("FBI"), and Director of the Orange County Regional Computer Forensics Laboratory, Orange, California ("OCRCFL").  The OCRCFL is a state of the art computer forensics laboratory comprised of task force officers from 15 agencies in Orange, Los Angeles, San Bernardino, and Riverside Counties.  The laboratory specializes in the archival, preservation, and analysis of items of digital evidence, including computers, mobile devices, removable media (thumb drives, CDs etc) and Audio/Video equipment.

2.   I have been a computer forensic examiner for the FBI since 2001, have attended 700+ hours of specialized training in computer/device forensics, and have certifications to conduct forensic analysis on Windows, Macintosh, and Linux/Unix systems, as well as mobile devices and cell phones.  I have been the Director of the OCRCFL since November of 2013.

3.   I have consulted extensively with the FBI's Cryptographic and Electronic Analysis Unit ("CEAU") in this matter, and bring their experience to bear in this declaration.

## II.  PURPOSE OF DECLARATION

4.   This declaration is made in support of an application for an order by the Court compelling Apple Inc. ("Apple") to assist the FBI in its effort to search of a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network ("SUBJECT DEVICE").

## III. SEIZURE AND EXAMINATION OF SUBJECT DEVICE

5.     The SUBJECT DEVICE was seized pursuant to the search warrant in Case No. ED 15-0451M, issued by the Honorable David T. Bristow, United States Magistrate Judge, on December 3, 2015.  The SUBJECT DEVICE was found inside of the SUBJECT VEHICLE identified in the warrant.  The underlying search warrant is attached hereto as Exhibit 1 and incorporated by reference.

6.     I know based on my participation in this investigation and conversations with other involved agents and San Bernardino County Information Technology personnel, that the search warrant arose out of an investigation into the December 2, 2015 shooting death of 14 people, and the shooting and injuring of 22 others, at the Inland Regional Center ("IRC") in San Bernardino, California, and the participation by Syed Rizwan Farook ("Farook") and his wife Tafsheen Malik ("Malik") in that crime.  Subsequent to the search warrant at issue, the FBI has obtained numerous warrants to search the digital devices and online accounts of Farook and Malik.  Through those searches the FBI has discovered, for example, that on December 2, 2015, at approximately 11:14 a.m., a post on a Facebook page associated with Malik stated, "We pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi," referring to Abu Bakr Al Baghdadi, the leader of Islamic State of Iraq and the Levant ("ISIL"), also referred to as the Islamic State ("IS"), or the Islamic State of Iraq and al-sham ("ISIS"), or Daesh.  ISIL, formerly known as Al-Qa'ida in Iraq ("AQI"), has been designated a foreign terrorist organization by the United States Department of State and has been so designated since December 2004.  Farook and Malik died later that same day in a shoot-out with law enforcement.

1    7.    The SUBJECT DEVICE is owned by Farook's employer at the
2  San Bernardino County Department of Public Health ("SBCDPH"), and
3  was assigned to, and used by, Farook as part of his employment.
4  While the SBCDPH does not have access to the passcode to the phone,
5  it has given its consent to the search of it and to Apple's
6  assistance with that search.

7    8.    The SUBJECT DEVICE is "locked" or secured with a numeric
8  passcode.  I have been very involved in the attempts to gain access
9  to the locked phone and comply with the search warrant.  With the
10 consent of the SBCDPH, I and other agents have been able to obtain
11 several iCloud backups for the SUBJECT DEVICE, and I am aware that a
12 warrant was executed to obtain from Apple all saved iCloud data
13 associated with the SUBJECT DEVICE.  I know from speaking with other
14 FBI agents that evidence in the iCloud account indicates that Farook
15 was in communication with victims who were later killed during the
16 shootings perpetrated by Farook on December 2, 2015.  In addition,
17 toll records show that Farook communicated with Malik using the
18 SUBJECT DEVICE between July and November 2015, but this information
19 is not found in the backup iCloud data.  Importantly, the most
20 recent backup is dated October 19, 2015, which indicates to me that
21 Farook may have disabled the automatic iCloud backup feature
22 associated with the SUBJECT DEVICE.  I believe this because I have
23 been told by SBCDPH that it was turned on when it was given to him,
24 and the backups prior to October 19, 2015 were with almost weekly
25 regularity.  I further believe that there may be relevant, critical
26 communications and data on the SUBJECT DEVICE around the time of the
27 shooting which has thus far not been accessed, may reside solely on
28 the SUBJECT DEVICE, and cannot be accessed by any other means known

to either the government or Apple. In addition, I have personally examined two other mobile devices belonging to Farook that were physically destroyed and discarded in a dumpster behind the Farook residence.

9. I have explored other means of obtaining this information with employees of Apple and with technical experts at the FBI, and we have been unable to identify any other methods feasible for gaining access to the currently inaccessible data stored within the SUBJECT DEVICE.

## IV. REQUESTED ASSISTANCE

10. I know based on my training and experience, knowledge of this case and review of Apple's publicly available information that the SUBJECT DEVICE is an iPhone 5c that was designed, manufactured, and sold by Apple. Apple also wrote and owns the software operating system marketed under the name of "iOS," and thus is the owner of the operating system for the phone at issue. Apple's software licensing agreement specifies that its software is "licensed, not sold," and otherwise prohibits users from transferring any ownership of the iOS software.

11. Apple strictly controls the hardware and software that is used to turn on and run its phones. According to Apple's "white papers" and other publicly available information about the security of its iOS programs, Apple has designed its mobile device hardware as well as its operating system software to only permit and run software that has been "signed" cryptographically by Apple using its own proprietary encryption methods. Apple has also added hardware-enforced features to the A6 processor found in the iPhone 5C which verifies software using Apple's cryptographic signature, ensuring

that Apple devices can only run verified/signed software during the booting process (when the phone is being turned on). These features prevent the government from running any other software on the SUBJECT DEVICE to attempt to recover data.

12. In addition, an iPhone 5c is encrypted by a combination of two components – one user-determined passcode, and one unique 256-bit Advanced Encryption Standard ("AES") key (referred to as a "UID") fused into the phone itself during manufacture. Both passcode components are required in combination for the phone to decrypt its contents. When a user inputs the user-determined passcode, the phone conducts a complex calculation as determined by Apple's software (and unknown to the government) which combines the UID with the user passcode. If the result is accurate, the data is decrypted.

13. If one does not know the user-determined passcode, it is possible, although time-consuming, to manually input passcodes one at a time until the passcode is determined. Apple, however, has also designed and written code for additional non-encryption-based features which the government cannot overcome on its own. First, Apple has designed a non-encryption, auto-erase function as part of its iOS, which destroys encryption key material required for decryption, and hence renders the contents of the device incapable of being decrypted after ten consecutive incorrect passcode attempts. If this erase function is enabled, iOS will instantly, irrecoverably, and without warning erase the encryption keys necessary for accessing stored data. Because iOS software must be cryptographically signed by Apple, only Apple is able to modify the iOS software to change the setting or prevent execution of the

function.   There is no way to know by examining the outside of the phone whether or not this function has been turned on in the SUBJECT DEVICE, although, in this instance, I suspect that it has because I am told by an employee of SBCDPH that the SUBJECT DEVICE was provided to Farook with the auto-erase function turned on, and I know from my review of the most recent backup from the iCloud that it showed the function turned on.

14.   Relatedly, Apple has designed and written code for another non-encryption based feature in that its iOS operating system is coded to invoke time delays which escalate after repeated, unsuccessful passcode entries.   This means that after each failed passcode entry, the user must wait a period of time before another attempt can be made.   From Apple documentation and testing, the time delays for the iPhone 5C are invoked by Apple software upon failed login attempts.   Apple documentation states that the software invokes no delay for the first four attempts; a 1-minute delay after the fifth attempt; a 5-minute delay after the sixth attempt; a fifteen minute delays after the seventh and eight attempt; and a 1-hour delay after the ninth attempt.   Additional wait times can also be added into the software.

15.   In order to allow the government to perform the search ordered in the warrant, and the ability to test passcodes to decrypt the SUBJECT DEVICE without unnecessary delay or fear that the data subject to search under the warrant would be rendered permanently inaccessible, the government requests that Apple be ordered to provide the FBI with a signed iPhone Software file, recovery bundle, or other Software Image File ("SIF") that can be loaded onto the SUBJECT DEVICE.   The SIF would load and run from Random Access

Memory ("RAM") and would not modify the iOS on the actual phone, the

user data partition or system partition on the device's flash

memory.   The SIF would be coded by Apple with a unique identifier of

the phone so that the SIF would only load and execute on the SUBJECT

DEVICE.   Since Apple's software currently has the capability to

query hardware for unique identifiers (serial numbers, ECID, IMEI,

etc.), the SIF could be created to only function on the SUBJECT

DEVICE, which would mitigate any perceived security risk to Apple

iOS software.   The SIF would be loaded via Device Firmware Upgrade

("DFU") mode, recovery mode, or other applicable mode available to

the FBI.   In addition, Apple could run the SIF from within its

facility, allowing passcodes to be tested electronically via remote

network connection.

    16.   Once active on the SUBJECT DEVICE, the SIF would have

three important functions: (1) the SIF would bypass or disable the

auto-erase function whether or not it has been enabled on the

SUBJECT DEVICE, meaning that multiple attempts at the passcode could

be made without fear that the data subject to search under the

warrant would be rendered permanently inaccessible; (2) the SIF

would enable the FBI to submit passcodes to the SUBJECT DEVICE for

testing electronically via the physical device port, Bluetooth, Wi-

Fi, or other protocol available on the SUBJECT DEVICE (meaning that

the attempts at the passcode would not have to be manually typed on

the phone's screen), or alternately, Apple could be given the phone

as is done when Apple recovers data from earlier iOS versions, but

provide the government remote access to the SUBJECT DEVICE through a

computer allowing the government to conduct passcode recovery

analysis.   This would allow the government to conduct the analysis

without Apple actually providing the government with the SIF; and (3) the SIF would not introduce any additional delay between passcode attempts beyond what is incurred by the Apple hardware.

17.  Based on my (and the CEAU's) review of available information about Apple's programs, Apple has the technological capability of providing this software without it being an undue burden.  Apple routinely patches security or functionality issues in its iOS operating system and releases new versions of its operating system to address issues.  I know from my training and experience, and that of my fellow agents, that providers of electronic communications services and remote computing services sometimes must write code in order to gather the information necessary to respond to subpoenas and other process, and that this is not a large burden.

18.  However, in an abundance of caution, the government also requests that the order permit Apple to satisfy the three goals of the SIF and the loading of the SIF onto the SUBJECT DEVICE in an alternative technical manner if mutually preferable.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on February 16, 2016, Riverside, California.

Christopher Pluhar
FBI Supervisory Special Agent

8

# EXHIBIT 1

ORIGINAL    UNDER SEAL

AO 93 (Rev. 12/09) Search and Seizure Warrant   (USAO CDCA Rev. 01/2013)

# UNITED STATES DISTRICT COURT
for the
Central District of California

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

Black Lexus IS300 California License Plate #5KGD203,
handicap placard 360466F, Vehicle Identification Number
JTHBD192X50094434

)
)
)
)  Case No. ED15-0451M
)
)
)

## SEARCH AND SEIZURE WARRANT

To:     Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____Central_____ District of _____California_____ *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-2

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before   _14 days from the date of its issuance_
*(not to exceed 14 days)*

☐ in the daytime  6:00 a.m. to 10 p.m.       ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge _on duty at the time of the return through a filing with the Clerk's Office._
*(name)*

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*  ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued:   _12/3/15, 2:27 A.M._        _____
                                                         *Judge's signature*

City and state:   Riverside, California            _David T. Bristow, U.S. Magistrate Judge_
                                                      *Printed name and title*

AUSA: AWC, MPT  MM

| Return | | |
|---|---|---|
| *Case No.:* | *Date and time warrant executed:* | *Copy of warrant and inventory left with:* |

*Inventory made in the presence of :*

*Inventory of the property taken and name of any person(s) seized:*

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

**Certification** (by officer present during the execution of the warrant)

*I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.*

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

AUSA: AWC, MPT *MS*

## ATTACHMENT A-2

## PROPERTY TO BE SEARCHED

Black Lexus IS300 California license plate #5KGD203, handicap

placard 360466F, vehicle identification number

JTHBD192X50094434.

INSTRUMENTALITY PROTOCOL

## I.   ITEMS TO BE SEIZED

1.   The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of (1) 18 U.S.C. § 844(d) (Transportation or Receipt of Explosive Devices with the Intent to Injure or Kill); (2) 18 U.S.C. § 844(i) (Attempted Destruction by Explosives of Any Building, Person, or Property); and (3) 18 U.S.C. § 844(n) (Conspiracy):

a.   Explosives, smokeless powder, black powder, gunpowder, or any other item that can be pipes, and wires;

b.   Pipes and any items that may cause fragmentation;

c.   Initiating devices to include burning fuse, hobby fuse, blasting caps, manual or electrical timers, dry cell batteries, electrical wire, alligator clips, electrical tape of assorted colors commonly used to secure exposed electrical wiring;

d.   Books related to the construction of explosives;

e.   Tools used in the construction of explosives such as include hand held vise grips, table mounted vise grips, pipe cutters, electrical; and non-electrical drills and drill bits.

f.   Address and/or telephone books, telephones, pagers, answering machines, customer lists, and any papers reflecting names, addresses, telephone numbers, pager numbers,

18

INSTRUMENTALITY PROTOCOL

fax numbers and/or identification numbers of sources of supply of explosives;

g.   No more than 5 documents and records, including electronic mail and electronic messages, reflecting the ownership, occupancy, possession, or control of the SUBJECT LOCATION, including lease/rental agreements, rent receipts, registration documents, bank records, utility bills, telephone bills, other addressed envelopes, and correspondence;

h.   Any digital device used to facilitate the above-listed violations and forensic copies thereof.

i.   With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i.   evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii.   evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

INSTRUMENTALITY PROTOCOL

as well as evidence of the presence or absence of security software designed to detect malicious software;

     iii. evidence of the attachment of other devices;

     iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

     v.   evidence of the times the device was used;

     vi.   passwords, encryption keys, and other access devices that may be necessary to access the device;

     vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

     viii.    records of or information about Internet Protocol addresses used by the device;

     ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2.   As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

INSTRUMENTALITY PROTOCOL

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3.  As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## II.  SEARCH PROCEDURE FOR DIGITAL DEVICES

4.  In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a.  Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at

INSTRUMENTALITY PROTOCOL

that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

INSTRUMENTALITY PROTOCOL

d.    If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e.    If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f.    If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g.    If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h.    The government may retain a digital device itself until further order of the Court or one year after the

23

conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

      i.    Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

      5.    In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

      a.    Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

      b.    Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

      c.    Any magnetic, electronic, or optical storage device capable of storing digital data;

INSTRUMENTALITY PROTOCOL

d.    Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e.    Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f.    Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g.    Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6.    The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

7.    The government is allowed to share the information obtained from this search (to include copies of digital media) with any government agency investigating, or aiding in the investigation of, this case or related matters.

25