SUPERIOR COURT OF THE STATE OF DELAWARE

| | | |
|---|---|---|
| JONATHAN RUDENBERG,<br><br>Petitioner Below,<br>Appellant<br><br>v.<br><br>DELAWARE DEPARTMENT OF JUSTICE, THE CHIEF DEPUTY ATTORNEY GENERAL & DELAWARE DEPARTMENT OF SAFETY AND HOMELAND SECURITY, DIVISION OF STATE POLICE,<br><br>Respondents Below,<br>Appellees. | ) | Case No. N16A-02-006 RRC |

**STATEMENT OF INTEREST OF THE UNITED STATES**

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

MARCIA BERMAN
Assistant Branch Director

CAROL FEDERIGHI
Senior Trial Counsel
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W. Room 7122
Washington, D.C. 20530
Tel.: (202) 514-1903
E-mail: carol.federighi@usdoj.gov

## TABLE OF CONTENTS

**PAGE**

## TABLE OF AUTHORITIES

**CASES** **PAGE(S)**



**FEDERAL STATUTES**

**STATE STATUTES**

## INTRODUCTION

In this action, petitioner Jonathan Rudenberg seeks to compel disclosure under the Delaware Public Records Act of sensitive information withheld by the Delaware State Police ("DSP") relating to its purchase and use of cell site simulator equipment. This submission by the United States is made pursuant to 28 U.S.C. § 517, which authorizes the Attorney General of the United States to send any officer of the Department of Justice to "attend to the interest of the United States in a suit pending in the court of the United States, or in the court of a State, or to attend to any other interest of the United States." Although the United States is not a party to this case, it has a direct interest in the protection of the information withheld by the DSP. Cell site simulator technology is a key tool in the Federal Bureau of Investigation's ("FBI's") investigation, interdiction, and suppression of criminal and terrorist activity. Disclosure of even minor details about this technology will jeopardize, if not vitiate, the ability of the FBI and the larger law enforcement community to successfully deploy this valuable technology to locate criminals and terrorists, and recover victims. And DSP's purchase and use of cell site simulator equipment is subject to a non-disclosure agreement with the FBI.

The information withheld by the DSP consists of sensitive, non-public information about the makes and models of cell site simulator systems and components parts and software purchased by DSP. Disclosure of this information could harm federal criminal and national security investigations by allowing criminals and terrorists to piece together information about cell site simulators' use and capabilities and thereby develop methods to evade them. Based on these concerns, courts have protected this type of information from disclosure, and this Court should do so as well. *See, e.g.*, *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012); *Rigmaiden v. Fed. Bureau of Investigation*, No. CV12-1605-DLR-BSB (D. Ariz.) (orders dated

Aug. 31, 2015 & Dec. 14, 2015); *People v. Michaels*, No. 5-140709-7 (Cal. Super. Ct., Contra Costa County) (orders dated Nov. 4, 2015 & Dec. 3, 2015); *Hodai v. City of Tucson*, 239 Ariz. 34, 365 P.3d 959 (Ariz. Ct. App. 2016).

As explained further below, the withheld information is exempt from disclosure under section 10002(*l*)(6) of the Delaware Freedom of Information Act ("Delaware FOIA"), Del. Code, tit. 29, § 10002(*l*)(6). That provision defines a "public record" subject to release under the Delaware FOIA as excluding "[a]ny records specifically exempted from public disclosure by statute or common law." *Id.* The information at issue here is exempted from public disclosure under both a federal statute and federal common law. First, the information at issue is exempted from release under the federal Freedom of Information Act, pursuant to exemption 7(E) of that Act. 5 U.S.C. § 552(b)(7)(E). Exemption 7(E) protects from public disclosure information that would reveal "techniques and procedures for law enforcement investigations or prosecutions" "if such disclosure could reasonably be expected to risk circumvention of the law." *Id.* The information at issue here is such information. Second, this sensitive information about cell site simulators would be protected from disclosure in criminal discovery under the "law enforcement sensitive" common-law privilege. The information at issue is protected by this privilege because it was supplied in confidence to the DSP regarding a sensitive law enforcement technique, and its disclosure could decrease the effectiveness of the investigative technique in future cases.

In sum, the redacted information falls within the scope of § 10002(*l*)(6). Accordingly, this Court should find that the DSP properly withheld the information at issue and should deny Rudenberg's petition seeking to compel disclosure of unredacted copies of the records at issue.

## BACKGROUND

### I. CELL SITE SIMULATORS

Law enforcement agents can use cell site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator operator's vicinity. Declaration of Russell D. Hansen, Supervisory Special Agent, currently assigned as the Chief, Tracking Technology Unit, FBI Operational Technology Division ("Hansen Decl."), ¶ 4. In general, cell site simulators function by transmitting as a cell tower, thereby simulating a cell tower. *Id.* ¶ 5. In response to the signals emitted by the simulator, cellular devices in the area of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower. *Id.*

A cell site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. Hansen Decl. ¶ 6. When used to locate a known cellular device, a cell site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. *Id.* Once the cell site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. *Id.* When used to identify an unknown device, the cell site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device. *Id.*

By transmitting as a cell tower, cell site simulators acquire the identifying information from cellular devices. Hansen Decl. ¶ 7. This identifying information is limited, however. *Id.* Cell site simulators provide only the relative signal strength and general direction of a subject

cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. *Id.* Moreover, cell site simulators used by federal, state, and local law enforcement agencies must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). Hansen Decl. ¶ 7. This includes any data contained on the phone itself: the cell site simulator does not capture emails, texts, contact lists, images, or other data from the phone, nor does it, as configured, provide subscriber account information (such as an account holder's name, address, or telephone number). *Id.*

Cell site simulator technology provides valuable assistance in support of law enforcement and public safety matters. Hansen Decl. ¶ 3. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate and rescue a kidnapped child, cell site simulators fulfill critical operational needs. *Id.* Cell site simulator technology is also an important tool in the federal government's effort to protect and defend the United States against terrorist and other threats to our national security. *Id.*

## II. LIMITS ON ACCESS TO CELL SITE SIMULATOR TECHNOLOGY

Federal law prohibits the use of any radio transmission equipment, which includes cell site simulator equipment, except as authorized by the Federal Communications Commission ("FCC"). *See* 47 U.S.C. §§ 301, 302a*; see also* 18 U.S.C. § 2512. Since 2010, the FCC has authorized manufacturers to sell cell site simulator equipment to state and local law enforcement agencies on two specific conditions: "(1) The making and sale of these devices shall be limited to federal, state, and local public safety and law enforcement officials only; and (2) state and local law enforcement agencies must [in] advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization." Hansen Decl. ¶¶ 9-10 & Exh. A.

This advance coordination has been accomplished through and documented by a non-disclosure agreement ("NDA") executed between the state or local law enforcement agency and the FBI. Hansen Decl. ¶ 10. The DSP signed such an NDA with the FBI in 2012. *Id.* ¶ 12 & Exh. B (FBI-DSP Non-Disclosure Agreement). Only upon execution of the NDA may a state or local agency purchase or otherwise acquire, use, or provide training about operating cell site simulator equipment. *Id.* ¶ 10. When a state or local law enforcement agency contacts one of the two authorized manufacturers about purchasing cell site simulator equipment, the manufacturer notifies the FBI about the agency's interest. *Id.* The FBI then contacts the agency to begin the coordination process, including the NDA. *Id.* Once the NDA is completed, the FBI notifies the manufacturer that the coordination has taken place. *Id.*

Through the NDAs, state and local law enforcement agencies stipulate that they will not disclose information about the technology and equipment and that they will notify the FBI upon receipt of any request for such information to provide the federal government the opportunity to protect the important federal equities at stake. Hansen Decl. ¶ 11. The NDA signed by DSP contained such a provision. *Id.* ¶¶ 12, 13. The NDA provides that the DSP "will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies." *Id.* ¶ 13 & Exh. B. In addition, the agreement provides that in the event that the DSP receives a request for such information pursuant to federal, state, or local law or in a court or administrative proceeding, it will immediately contact the FBI in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels. Hansen Decl., Exh. B ¶¶ 7, 11.

## III. RUDENBERG'S DELAWARE FOIA REQUEST

On May 15, 2015, Rudenberg submitted a request to the Delaware State Police pursuant to the Delaware FOIA, Del. Code tit. 29, §§ 10001-10007, for records related to the acquisition and use of cell site simulators by the DSP. *See* Appellant's Opening Br. ("Rudenberg Br.") 5 & Exh. A thereto. The request contains nine subparts, seeking, *inter alia*, records relating to: (1) the DSP's acquisition of cell site simulators, including invoices, purchase orders, and similar documents; (2) any agreements between the DSP and other law enforcement agencies to share the use of cell site simulators; (3) any pertinent non-disclosure agreements; (4) DSP policies and guidelines governing the use of cell site simulators; (5)-(6) any agreements with wireless service providers or communications, licenses, or agreements with the FCC or the Delaware Public Service Commission; and (7)-(9) the number of investigations in which cell site simulators have been used by the DSP, a list of cases in which cell site simulators were used as part of the underlying investigation, and any applications for warrants or court orders authorizing the use of cell site simulators. *Id.*; *see also* Appellee's Opening Br. ("DSP Br.") 1-3.

On June 5, 2015, the Delaware State Police responded to the request by stating that the records could not be divulged pursuant to the FBI-DSP NDA. DSP Br. 3. On June 17, 2015, Rudenberg filed a petition for review of this response with the Chief Deputy Attorney General, pursuant to section 10005(b) of the Delaware FOIA, Del. Code tit. 29, § 10005(b). DSP Br. 3.

In the meantime, the DSP brought Rudenberg's request and this suit to the FBI's attention in compliance with the NDA it had previously signed with the FBI. Hansen Decl. ¶ 19. The FBI began working with the DSP to identify information that can be released without risking harm to law enforcement and national security interests. *Id.* Among the records that DSP had identified as responsive to Rudenberg's request are ten pages of purchase orders and invoices

related to DSP's acquisition of CSS systems and training. DSP Br. 15-16. After consultation with the FBI, DSP redacted from these pages the makes and model numbers of the cell site simulator equipment and the component parts and software necessary to configure CSS systems. Hansen Decl. ¶ 19. The FBI has assessed that disclosure of this information to the public would pose significant risks to effective law enforcement, and ultimately to the safety of the public and the national security of the United States. *Id.* ¶ 20.

The Chief Deputy Attorney General ("CDAG") issued her decision in Rudenberg's appeal on December 29, 2015. DSP Br. 4. The CDAG found that the non-disclosure agreement between the DSP and the FBI was subject to disclosure and ordered DSP to release that agreement (which DSP did). *Id.* She also directed DSP to release the redacted purchase order records (discussed in the previous paragraph), which DSP also did. *Id.* at 4-5.

On February 26, 2016, Rudenberg appealed the Chief Deputy's decision to this Court, pursuant to § 10005(b) of the Delaware FOIA. DSP Br. 5. In this appeal, Rudenberg challenges, *inter alia*, the redactions made to the purchase order records, arguing that he is entitled to information concerning the specific model names. Rudenberg Br. 22-23.

## ARGUMENT

### THE REDACTED INFORMATION IS EXEMPT FROM DISCLOSURE UNDER DELAWARE FOIA SECTION 10002(*l*)(6)

Section 10002(*l*)(6) of the Delaware FOIA defines a "public record" subject to release as excluding "[a]ny records specifically exempted from public disclosure by statute or common law." Del. Code, tit. 29, § 10002(*l*)(6); *see generally Guy v. Judicial Nominating Comm'n*, 659 A.2d 777, 783 (Del. Super. 1995) (adopting a broad meaning of word "statute" in specifically holding that "the word 'statute' within the meaning of this exemption under the Act is sufficiently inclusive to embrace provisions of the State Constitution"). As discussed further

below, the information at issue here, specifically, the makes and model numbers of cell site simulators purchased by DSP, and information regarding component parts and software, is protected both under a federal statute – the federal FOIA – and under federal common law – the law enforcement sensitive privilege. Accordingly, this information is exempt from disclosure under Delaware's FOIA and was properly redacted from the purchase orders.

### A. The Redacted Information is Specifically Exempted From Disclosure by the Federal FOIA, 5 U.S.C. § 552

Under the federal FOIA, records or information compiled for law enforcement purposes are not subject to public disclosure when such disclosure would reveal "techniques and procedures for law enforcement investigations or prosecutions, or would [reveal] guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). Pursuant to this exemption, federal courts have protected non-public details about a wide variety of commonly known law enforcement techniques and procedures. *See* The United States Department of Justice Guide to the Freedom of Information Act, Exemption 7(E) at p. 6-9, https://www.justice.gov/oip/doj-guide-freedom-information-act-0 (compiling cases standing for the proposition that non-public details about publicly-known techniques and procedures, such as surveillance, are covered by Exemption 7(E) because disclosure of such could reduce or nullify the effectiveness of the techniques and procedures); *see ,e.g., Kurdyukov v. U.S. Coast Guard*, 657 F. Supp. 2d 248, 257 (D.D.C. 2009) ("An agency may withhold information from disclosure where, as here, it would provide insight into its investigatory or procedural techniques."); *Fisher v. U.S. Dep't of Justice*, 772 F. Supp. 7, 12 (D.D.C. 1991) (upholding FBI's decision to withhold information about law enforcement techniques where disclosure "could alert subjects in drug investigations about techniques used to aid the FBI"), *aff'd*, 968 F.2d 92 (D.C. Cir. 1992).

As described above, cell site simulators are a key tool in the investigation, interdiction, and suppression of criminal and terrorist activity. Hence, information about this technology falls within the purview of Exemption 7(E). Such information is protected because, as explained by William Hansen, current Chief of the Tracking Technology Unit in FBI's Operational Technology Division, disclosure of even minor details about cell site simulators can reasonably be expected to provide adversaries – criminals and terrorists alike – with the ability to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to circumvent the law. Hansen Decl. ¶ 22. Disclosure of the information at issue here (make and model information and information regarding software updates, component parts, and training manuals from purchase orders) would reveal the relative capabilities – and corresponding limitations – of DSP to electronically surveil and locate criminals and terrorists, and rescue/recover crime victims because it would reveal the specific resources available to the police department (as well as those not available to it). *Id.* ¶ 23.a. Disclosure of this information would not only implicate the equities and safety of the community in Delaware. *Id.* Combined with other information that may be available to criminals and terrorists concerning other jurisdictions, disclosure of make and model information used by the DSP would permit the development and honing of "heat maps" identifying the areas in the country where particular technology and resources are utilized by law enforcement and where they are not – *i.e.*, those areas where criminals and terrorists can operate without fear of detection by cell site simulator technology and those areas where they need to modify their behaviors (or that they need to avoid) because the likelihood that law enforcement will be able to locate them is greater. *Id.* Thus, the information at issue in this category not only reflects on the resources that DSP can bring to bear in its cases, but also adds critical information to the fund already available for

criminals and terrorists to use in order to strategically navigate and thwart law enforcement on a broad scale. *Id.*

Furthermore, disclosure of listings of particular components necessary to configure particular systems would also reveal tradecraft information about platforms and modes of operation of CSS equipment. Hansen Decl. ¶ 23.b. Because this information would reveal not only the platforms and modes on which DSP operates its gear specifically, but also the tradecraft capabilities of others using the gear including federal law enforcement agencies, disclosure of this information would permit criminals and terrorists across the country to devise strategies to avoid the reach of the gear, develop technological countermeasures, and otherwise thwart the technology in order to circumvent local, state, and federal law. *Id.*

Accordingly, the information at issue here would be exempt from release under FOIA Exemption 7(E). Rudenberg asserts that the information he sought in his request has "routinely" been ordered to be disclosed under the federal FOIA, citing *American Civil Liberties Union v. United States Department of Justice*, No. 13-cv-03127-MEJ, 2015 WL 3793496 (N.D. Cal. June 17, 2015), and *American Civil Liberties Union v. United States Department of Justice*, 655 F.3d 1, 19 (D.C. Cir. 2011). Rudenberg Br. 5. He is wrong – the type of information about cell site simulators that the FBI seeks to protect here has not been ordered disclosed in federal FOIA cases, let alone on a routine basis. *See Rigmaiden v. Fed. Bureau of Investigation*, No. 2:12-cv-01605-DLR-BSB (D. Ariz.) (orders dated Aug. 31, 2015 & Dec. 14, 2015) (attached as Exhibits A and B to Federighi Decl.). First, in the District of Columbia case cited by Rudenberg, the court rejected the government's assertion of Exemptions 6 and 7(C) and directed the government to produce "*docket information* from criminal cases in which the government prosecuted individuals after judges granted applications for cell phone location data without determining

probable cause, and in which those individuals were ultimately convicted or entered public guilty pleas." *ACLU v. U.S. DOJ*, 655 F.3d at 19-20 (emphasis added). The holding of the case thus did not concern technical or make/model information about cell site simulators, or even the application of Exemption 7(E).

In the California case cited by Rudenberg, at issue ultimately were legal templates for applications and proposed orders related to cell site simulators; legal guidance memoranda regarding use of cell site simulators; an excerpt from the USA Book; and a sealed search warrant, application, and affidavit. *ACLU v. DOJ*, 2015 WL 3793496, at *2. The district court did conclude that DOJ's assertion of Exemption 7(E) to protect documents drafted by legal advisors and a reference document prepared to assist prosecutors and law enforcement agents was insufficient. *Id*. at *11. However, the information at issue was not the same as the type of technical information that the FBI seeks to protect here. In any event, to the extent that there is some similarity between the information in the two cases, this single decision finding that DOJ had not met its burden to protect such information under Exemption 7(E) does not demonstrate that courts "routinely" order disclosure under the federal FOIA of the types of information the FBI seeks to protect. *See also Hodai*, 365 P.3d at 964-66 (applying balancing test to find that the Tucson Police Department properly withheld cell site simulator training materials in response to a request under the Arizona Public Records Act, concluding that statement of FBI agent that "knowledge of how the equipment works 'could easily lead to the development and employment of countermeasures' . . . is not merely a possible harm based on a hypothetical situation, but one rooted in experience").

In sum, the information redacted from the purchase orders is exempt from disclosure pursuant to Exemption 7(E) of the federal FOIA. As a result, the information is therefore exempt

from disclosure under § 10002(*l*)(6) of the Delaware FOIA as information "specifically exempted from public disclosure by statute."

### B. The Redacted Information is Specifically Exempted From Disclosure by the Common Law Under the Law Enforcement Privilege

In addition to falling with the federal FOIA exemption 7(E), information about cell site simulators is confidential, privileged information that is protected from disclosure in criminal discovery under the "law enforcement sensitive" privilege. Accordingly, it falls within the scope of § 10002(*l*)(6) for this reason as well.

The "law enforcement sensitive" privilege applies in criminal cases to protect information where disclosure of that information would allow criminal defendants and others to ascertain law enforcement's capabilities and limitations in this area, and thus to develop countermeasures. *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 992 (D. Ariz. 2012) (federal criminal prosecution); *United States v. Garey*, No. 5:03-CR-83, 2004 WL 2663023 (M.D. Ga. Nov. 15. 2004) (same). The "law enforcement privilege" balances the defendant's need for the information against the public interest in confidentiality. *Rigmaiden*, 844 F. Supp. 2d at 988-89. The privilege applies to the information at issue here because, as the FBI Program Manager avers, public knowledge of this information could jeopardize the effectiveness of the use of cell site simulators as an investigative tool. Hansen Decl. ¶¶ 20-23. Although some general information about cell site simulators and their operation is publicly available, the specific capabilities, settings, limitations, tradecraft, and other types of information withheld here have not been authoritatively disclosed or confirmed by the FBI. *Id.* ¶ 25. As explained above, disclosure of this information would therefore add critical information to the fund already available for criminals and terrorists to use in order to strategically navigate and thwart law enforcement on a broad scale. *Id.*

The federal courts have found that information regarding cell site simulators is protected by this "law enforcement sensitive" privilege. In *Rigmaiden*, based on the testimony of an FBI Supervisory Special Agent, the court found that the privilege applied to "the precise equipment used by the FBI and the precise manner in which it was used," including information such as the manufacturer model information, instructions, user manuals and other technical and operational information. 844 F. Supp. 2d at 993-94. The court concluded that disclosure of this information "would enable adversaries of law enforcement to defeat electronic surveillance operations and to avoid detection by such surveillance" and therefore "would compromise the ability of the FBI and other law enforcement agencies to combat crime." *Id.* at 994; *see also id.* at 1002 ("Disclosure of the specific equipment used by the government . . . would hamper future law enforcement efforts . . . ."), 1004. *Accord United States v. Garey*, No. 5:03-CR-83, 2004 WL 2663023, *4 (M.D. Ga. Nov. 15, 2004) (upholding the assertion of investigative privilege with respect to information regarding the cell site simulator equipment employed during a criminal investigation).

At least one state court has found similar material protected by a similar state-law privilege. *See People v. Michaels*, No. 5-140709-7 (Cal. Super. Ct., County of Contra Costa) (orders dated Nov. 4, 2015 & Dec. 3, 2015) (attached as Exhs. C & D to Federighi Decl.) (state criminal prosecution). In *Michaels*, criminal defendants sought pretrial discovery relating to the use of cell site simulators, and the State opposed the discovery request asserting that the information was protected by the official government privilege under California Evidence Code 1040. California's "official information" privilege protects non-public, confidential information from disclosure when disclosure is "against the public interest." Cal. Evid. Code § 1040(b)(2). Based on testimony presented by an FBI Supervisory Special Agent, the Superior Court held that

the following information was protected: "[t]he make, model, manufacturer, technical specifications, and capabilities of the particular cell site simulator device used in this investigation; the specific techniques employed in operating the cell site simulator in this investigation; and the names and identities of the individual agents who operated the cell site simulator in this investigation." Order dated Nov. 4, 2015, at 8. As the court explained, "disclosure of this information would enable those suspected of crimes and fugitives from justice to avoid or defeat the efficacy of the cell site simulator" and thus "compromise the ability of law enforcement officers to investigate, solve, prosecute, and prevent crimes." *Id.* at 8-9. Thus, "disclosure of the information listed above would be against the public interest because there is a necessity for preserving the confidentiality of this information that outweighs the necessity for disclosure to the Defendants in the interest of justice." *Id.* at 8.

In sum, the information that DSP protected here at the FBI's request falls within the categories of sensitive law enforcement information that have been found privileged in federal and state courts, and thus that have been exempted from disclosure. Accordingly, this information is "specifically exempted from public disclosure by . . . common law" and exempt from disclosure under § 10002(*l*)(6) of the Delaware FOIA for this reason as well.

## CONCLUSION

For all the foregoing reasons, the United States respectfully requests that the Court find that the DSP properly withheld the information described above and deny Rudenberg's appeal.

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

MARCIA BERMAN
Assistant Branch Director

*s/Carol Federighi*
CAROL FEDERIGHI
Senior Trial Counsel
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W. Room 7122
Washington, D.C. 20530
Tel.: (202) 514-1903
E-mail: carol.federighi@usdoj.gov

Dated: September 27, 2016