



SUPERIOR COURT OF THE STATE OF DELAWARE

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

---

**DECLARATION OF RUSSELL D. HANSEN**

I, Russell D. Hansen, declare as follows:

(1) I am a Supervisory Special Agent (“SSA”) with the Federal Bureau of Investigation (“FBI”), currently assigned as the Chief, Tracking Technology Unit, Operational Technology Division (“OTD”) in Quantico, Virginia. I am over the age of 18 years and without legal disability, and if called as a witness could competently testify to the facts set forth below. I have been employed as an FBI Special Agent since 1997. As Unit Chief, I am responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of all FBI investigative, intelligence collection, and operational programs. I am responsible for establishing and advising on policy guidance for the FBI, including whether a particular tool or technique my program manages meets the criteria for protection as law enforcement sensitive, while ensuring that state-of-the-art technical investigative assets remain available to field technical programs to enable them to assist in a wide range of technical investigative missions. This includes the use and

deployment of electronic surveillance devices such as cell site simulator/pen register trap and trace systems.

(2) Due to the nature of my official duties, I am familiar with the matters at issue in this case. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

**BACKGROUND INFORMATION ABOUT CELL SITE SIMULATORS AND  
THE FEDERAL GOVERNMENT SHARING THE TECHNOLOGY  
WITH STATE AND LOCAL LAW ENFORCEMENT PARTNERS**

(3) Cell site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell site simulators fulfill critical operational needs. Cell-site simulator technology is also an important tool in the Federal Government's efforts to protect and defend the United States against terrorist and other threats to our national security. Indeed, cell site simulators are defense articles on the U.S. Munitions List and thus are prohibited from export under the International Traffic In Arms Regulations ("ITAR") without a license from the Department of State. *See* 22 C.F.R. §§ 120.1 – 130.17 (ITAR); 22 C.F.R. § 121.1, U.S. Munitions List Category XI(b).<sup>1</sup> Moreover, technical data about Category XI(b) defense articles, including cell site simulators, is also regulated and cannot be exported without a license pursuant to 22 C.F.R. § 121.1, Category XI(d). Technical data is "[i]nformation ... which is required for the design, development, production,

---

<sup>1</sup> Effective December 29, 2015, Category XI(b) consists of "[e]lectronic systems or equipment ... specially designed for intelligence purposes that collect, survey, monitor, or exploit the electromagnetic spectrum (regardless of transmission medium), or for counteracting such activities." 80 Fed. Reg. 37975-76 (Jul. 2, 2015).

manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles.” 22 C.F.R. § 120.10(a)(1).

(4) 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. This technology is one tool among many traditional law enforcement techniques available to law enforcement.

(5) In general, cell site simulators function by transmitting as a cell tower.<sup>2</sup> In response to the signals emitted by the simulator, cellular devices in the proximity 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.

(6) A cell site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. 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. 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. 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.

---

<sup>2</sup> Lay persons often use the term “IMSI catchers” interchangeably with the term “cell site simulator.” DOJ considers these to be two different capabilities. DOJ policy describes cell site simulators as equipment that “function[s] by transmitting as a cell tower.” See “DOJ Policy Guidance: Use of Cell-Site Simulator Technology” (Sept. 3, 2015), available at <http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators>. On the other hand, an IMSI catcher need not transmit to accomplish its function (*i.e.*, passive signaling data collection).

(7) By transmitting as a cell tower, cell site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. 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. 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). This includes any data contained on the phone itself. The cell site simulator does not remotely capture e-mails, 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).

(8) Use of cell site simulators is predicated on obtaining a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure or the applicable state equivalent unless an exception exists.<sup>3</sup>

(9) Cell site simulator/pen register technology was originally developed under contract with the Federal Government. The United States has authorized two private companies to manufacture this equipment and since 2010 has conditioned their ability to sell the equipment to state, and local law enforcement agencies under specific and controlled terms reflecting its sensitive nature.<sup>4</sup>

---

<sup>3</sup> The U.S. Department of Justice's policy on cell site simulator use recognizes two exceptions: exigent circumstances that vitiate the Fourth Amendment's warrant requirement, and exceptional circumstances where exigent circumstances do not exist but the law nevertheless does not require a warrant and obtaining a search warrant is impracticable. In either circumstance, law enforcement officials are nevertheless expected to comply with the Pen Register Statute, 18 U.S.C. § 3121 *et seq.*

<sup>4</sup> Some state and local law enforcement agencies acquired cell site simulator equipment before institution of the requirement to coordinate and execute non-disclosure agreements with the FBI. *See, e.g., Hodai v. City of*

(10) Federal law prohibits the use of any radio transmission equipment, except as authorized by the Federal Communications Commission (“FCC”). Cell site simulator equipment is radio transmission equipment. The FCC has issued authorization for manufacturers to sell their equipment to state and local law enforcement agencies with two conditions: (1) the marketing and sale of cell site simulator devices is limited to Federal, state, and local public safety and law enforcement agencies; and (2) state and local agencies must coordinate with the FBI in advance of their acquisition and use of the equipment. *See* FCC Grant of Equipment Authorization to Harris Corp., dated March 2, 2012 (Exhibit A hereto). This advance coordination is accomplished through and documented by a Non-Disclosure Agreement (“NDA”) executed between the state or local law enforcement agency and the FBI. 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 from either of the two previously-referenced companies. Thus, when a state or local law enforcement agency contacts one of these manufacturers about purchasing such equipment, the manufacturer notifies the FBI about the agency’s interest. The FBI then contacts the agency to begin the coordination process, including the NDA. Once the NDA is completed, the FBI notifies the manufacturer that the coordination has taken place.

(11) 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.

---

*Tucson and Tucson Police Dep’t*, Case No. C2014225, slip op. at 7 (Ariz. Sup. Ct., Pima County December 11, 2014).

(12) As relevant here, the Delaware State Police (“DSP”) signed an NDA with the FBI as a prerequisite to purchasing its cell site simulator systems. The NDA between the FBI and DSP provides:

Disclosing the existence of and the capabilities provided by [cell site simulator equipment and technology] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI’s inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that [cell site simulator equipment and technology] continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public.

*See Exhibit B hereto (FBI-DSP Non-Disclosure Agreement).*

(13) In addition, by executing the NDA, DSP agreed that it “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 descriptions(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies,” and that “[i]n the event that [DSP] receives a request pursuant to the Freedom of Information Act (5 U.S.C. 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related

documentation (including its technical/engineering description(s) and capabilities), the [DSP] will immediately notify the FBI to seek to prevent disclosure through appropriate channels.”

**RUDENBERG’S DELAWARE FREEDOM OF INFORMATION ACT REQUEST**

(14) On May 15, 2015, Rudenberg submitted a request under Delaware’s Freedom of Information Act (“Delaware FOIA”) to DSP for information concerning its use of cell site simulators. Specifically, he requested nine categories of information, including purchase records; sharing agreements with other agencies; NDAs; policies and guidelines regarding CSS use; communications with wireless service providers, the FCC, and the Delaware Public Service Commission; numbers and lists of cases in which cell site simulators were used; and applications for court orders to use cell site simulators.

(15) On June 5, 2015, DSP denied the request, citing the FBI-DSP Non-Disclosure Agreement (“NDA”).

(16) Rudenberg then submitted a petition challenging that decision to the Chief Deputy Attorney General of Delaware on June 17, 2015, pursuant to the Delaware FOIA.

(17) On December 29, 2015, the Chief Deputy issued her decision, as a result of which DSP disclosed the NDA as well as redacted versions of certain purchase documents that it had previously offered to release in redacted form.

(18) On February 26, 2016, Rudenberg appealed the Chief Deputy’s decision in Delaware Superior Court pursuant to the Delaware FOIA.

(19) The records that DSP processed and released in part to Rudenberg consist of ten pages of purchase orders and invoices related to DSP’s acquisition of CSS systems and training. The FBI requested that DSP redact from these pages the names and model numbers of the cell

site simulator equipment and the component parts and software necessary to configure CSS systems.

(20) 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. Accordingly, the FBI concluded that this information needs to be protected in furtherance of public safety and national security.

#### **RISK OF HARM FROM DISCLOSURE**

(21) The Federal Government, including but not limited to the FBI, has a strong interest in protecting from disclosure technical and operational information about cell-site simulators and their use. Accordingly, the FBI protects information about this equipment and associated techniques from disclosure. The FBI directs its agents that, while the product of an identification or location operation may be disclosed (*e.g.*, that a suspect was apprehended or a victim recovered at a particular location), neither the details of the equipment's operation nor the tradecraft involved in its use may be disclosed. In the federal Freedom of Information Act ("Federal FOIA") context, the FBI protects such information pursuant to Federal FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E). Additionally, the Federal Government asserts the law enforcement privilege in discovery to shield such information, because disclosure would allow criminal defendants and others to ascertain law enforcement's capabilities and limitations in this area, and thus to develop countermeasures. *See, e.g., U.S. v. Rigmaiden*, 844 F.Supp.2d 982 (D. Ariz. 2012) (federal criminal prosecution); *U.S. v. Garey*, 2004 WL 2663023 (M.D. Ga. Nov. 15, 2004) (same). *Accord California v. Michaels*, Case No. 5-140709-7 (Sup. Ct. of the State of Calif., County of Contra Costa) (Orders dated Nov. 4, 2015 and Dec. 3, 2015) (state criminal prosecution applying "official information" privilege under California Evidence Code § 1040 to protect CSS information based on testimony by FBI Supervisory Special Agent); *Hodai v. City*



*of Tucson & Tucson Police Dep't*, Case No. C20141225 (Sup. Ct. of AZ, Pima County) (Ruling dated Dec. 11, 2014) (state public records litigation where the court held that information about cell site simulators was exempt from disclosure based on the law enforcement privilege), *on appeal* Case No. 2 CA-CV 2015-0018 (AZ Ct. of Appeals). It is just as imperative for this information to be protected in response to requests under state information access statutes.

(22) In particular, CSS equipment is a key tool in the investigation, interdiction, and suppression of criminal and terrorist activity and threats to the national security of the United States. Disclosure of even minor details about cell site simulators may cause harm to law enforcement efforts and the national security of the United States because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance itself. Thus, disclosure of what appears to be innocuous information about cell site simulators may provide adversaries (criminals and terrorists alike) with information about the capabilities, limitations, and circumstances of the equipment's use, and would allow such adversaries to accumulate information and draw conclusions about the use and technical capabilities of the technology. In turn, this would provide them with the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of the technology in order to evade detection by law enforcement and circumvent the law. Adversaries and others could also use such information to disrupt and dismantle the functioning of the equipment altogether, thus rendering it nonfunctional and obviating its utility in any circumstances. Indeed, internet bloggers are already outlining ways to try to circumvent the Federal Government's cellular locating and identifying capabilities. Rendering this technology obsolete would seriously undermine the criminal law enforcement efforts of Federal, state, and local law enforcement agencies

nationwide, as well as the efforts of the Federal Government to protect and safeguard the national security of the United States.

(23) DSP identified responsive information in various records related to its procurement and purchase of CSS equipment and component parts, software, and training. The FBI asked DSP to protect CSS make and model information in these records. The risk of harm from disclosing this information follows.

a. Disclosure of this information, on its own, would reveal the relative capabilities – and correspondingly, 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). But disclosure of this information would not only implicate the equities and safety of the community in Delaware. Combined with other information, disclosure of this information would permit the development and honing of “heat maps” identifying the areas where particular technology and resources are utilized by law enforcement – *i.e.*, 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. 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.

b. 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. 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.

(24) The FBI cannot publicly provide any greater specificity in the descriptions of the information protected, the reasons for protecting that information, or the risks of harm faced by its disclosure without disclosing the very information we have sought to protect, and thereby causing the harms we seek to prevent. However, the FBI is prepared to provide more detailed testimony on an *in camera, ex parte* basis to the Court should it determine that such a briefing would assist it in resolution of this matter.

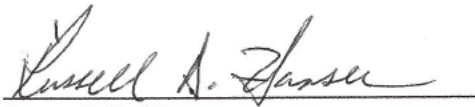
### CONCLUSION

(25) As discussed above, the Federal Government has a significant interest in ensuring that cell site simulator technology remains a viable tool in enforcing criminal laws and protecting the security of the United States. Given the media attention to cell site simulators, the inability to control the unauthorized release of information in the internet age, and the ready access that criminals and terrorists have to any information published on the internet about this (and other) vital law enforcement techniques, disclosure of the information at issue in this case will jeopardize, if not vitiate, the FBI and larger law enforcement community's ability to successfully deploy this valuable technology to locate criminals and terrorists, and recover victims. Although some information about cell site simulators and their operation is publicly available, the specific capabilities, settings, limitations, tradecraft, and other types of information discussed herein have

not been authoritatively disclosed, confirmed, or refuted by the FBI. Therefore, if such information is disclosed or endorsed here, criminal defendants and terrorists will gain valuable intelligence on the specific capabilities of the law enforcement community at large to effect surveillance of and locate individuals, which they can then use to effectively and successfully circumvent the law and/or disrupt or dismantle the equipment. Finally, much of this information is regulated under the ITAR and cannot be exported without a license.

Pursuant to 28 U.S.C. 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 27<sup>th</sup> day of September, 2016 in Quantico, Virginia.



Russell D. Hansen  
Operational Technology Division  
Federal Bureau of Investigation

# **EXHIBIT A**

**COPY**

FEDERAL COMMUNICATIONS  
COMMISSION  
WASHINGTON, D.C. 20554

**COPY**

GRANT OF EQUIPMENT  
AUTHORIZATION  
Certification

Harris Corporation  
Government Communications Systems Div PO  
Box 91000  
Melbourne, FL 32902  
United States

Date of Grant: 03/02/2012

Application Dated: 01/10/2012

**Attention: Stanley Gutowski , WPG Chief Systems Engineer**

**NOT TRANSFERABLE**

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: NK73092523

Name of Grantee: Harris Corporation

Equipment Class: PCS Licensed Transmitter

Notes: Mobile Cellular Transceiver System

Modular Type: Does not apply

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	22H	869.2 - 893.8	0.229	0.2 PM	300KGXW
	24E	1930.2 - 1989.8	0.186	0.2 PM	300KGXW
	22H	870.25 - 893.75	0.195	0.2 PM	1M25F9W
	24E	1931.25 - 1988.75	0.076	0.2 PM	1M25F9W
	22H	871.4 - 891.6	0.214	0.9 PM	4M80F9W
	24E	1932.4 - 1987.6	0.082	2.0 PM	4M80F9W
	90	851.025 - 865.975	0.122	1.9 PM	12K5GXW

(1) The marketing and sale of these devices shall be limited to federal, state, local public safety and law enforcement officials only; and (2) State and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.

Output power is conducted. Device complies with mobile exposure requirements of 2.1091.

**Mail To:**  
**Stanley Gutowski,**  
**Harris Corporation**  
**9800**  
**Melbourne, FL 32902**

**EA175543**

# **EXHIBIT B**



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

May 23, 2012

Robert Coupe  
Colonel  
Delaware State Police  
1441 N. DuPont Highway  
Dover, DE 19903

Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations

*LAW ENFORCEMENT SENSITIVE (LES): The information in this document is the property of the Federal Bureau of Investigation (FBI) and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI Operational Technology Division authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network.*

Dear Colonel Coupe:

We have been advised by Harris Corporation of the Delaware State Police's request for acquisition of certain wireless collection equipment/technology manufactured by Harris Corporation. Consistent with the conditions on the equipment authorization granted to Harris Corporation by the Federal Communications Commission (FCC), state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.

As you are aware, law enforcement agencies increasingly rely on wireless collection equipment/technology to conduct lawfully-authorized electronic surveillance. Disclosing the existence of and the capabilities provided by such equipment/technology to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is,



UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE

disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings. Accordingly, the Delaware State Police agrees to the following conditions in connection with its acquisition and use of the Harris Corporation equipment/technology:

1. By entering into this agreement, the Delaware State Police affirms that it has statutory authority to lawfully employ this technology and will do so only in support of public safety operations or criminal investigations.
2. The Delaware State Police assumes responsibility for operating the equipment/technology in accordance with Federal law and regulation and accepts sole liability for any violations thereof, irrespective of the Federal Bureau of Investigation approval, if any, for the sale of the equipment/technology.
3. The Delaware State Police will ensure that operators of the equipment have met the operator training standards identified by the FBI and are certified to conduct operations.
4. The Delaware State Police will coordinate with the FBI in advance of its use of the wireless collection equipment/technology to ensure de-confliction of respective missions.
5. The Delaware State Police 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.
6. The Delaware State Police 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) provided to it to any other law enforcement or government agency without the prior written approval of the FBI. Prior to any approved distribution, dissemination, or comparable disclosure of any information concerning the wireless collection equipment/technology or any software, manuals, or related technical documentation related to such equipment/technology, all materials shall be marked "Law Enforcement Sensitive, For Official Use Only - Not to be Disclosed Outside of the Delaware State Police."
7. The Delaware State Police shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related

UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE

Page 2 of 5

000031

documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI. If the Delaware State Police learns that a District Attorney, prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology in a manner that will cause law enforcement sensitive information relating to the technology to be made known to the public, the Delaware State Police will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.

Notification shall be directed to the attention of:

Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

8. In addition, the Delaware State Police will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology. This point supposes that the agency has some control or influence over the prosecutorial process. Where such is not the case, or is limited so as to be inconsequential, it is the FBI's expectation that the law enforcement agency identify the applicable prosecuting agency, or agencies, for inclusion in this agreement.
9. A copy of any court order in any proceeding in which the Delaware State Police is a party directing disclosure of information concerning the Harris Corporation equipment/technology and any associated software, operating manuals, or related

documentation (including its technical/engineering description(s) and capabilities) will immediately be provided to the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise. Any such court orders shall be directed to the attention of:

Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

10. The Delaware State Police will not publicize its acquisition or use of the Harris Corporation equipment/technology or any of the capabilities afforded by such equipment/technology to the public, other law enforcement agencies, or other government agencies, including, but not limited to, in any news or press releases, interviews, or direct or indirect statements to the media.
11. In the event that the Delaware State Police receives a request pursuant to the Freedom of Information Act (5 U.S.C. § 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities), the Delaware State Police will immediately notify the FBI of any such request telephonically and in writing in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels. Notification shall be directed to the attention of:


Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod A  
Quantico, Virginia 22135  
(703) 985-6100

and

Unit Chief  
Tracking Technology Unit  
Operational Technology Division  
Federal Bureau of Investigation  
Engineering Research Facility  
Building 27958A, Pod B  
Quantico, Virginia 22135  
(703) 985-6840

The Delaware State Police's acceptance of the above conditions shall be evidenced by the signatures below of an authorized representative and wireless collection equipment operators of the Delaware State Police.

Sincerely,

  
\_\_\_\_\_  
Amy S. Hess  
Assistant Director  
Operational Technology Division  
Federal Bureau of Investigation

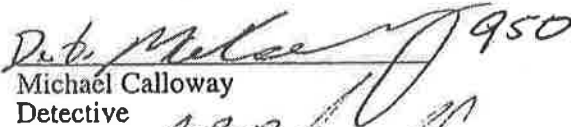
Acknowledged and agreed to this 31<sup>ST</sup> day of MAY, 2012.



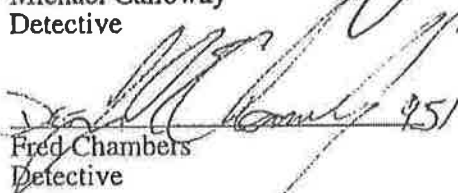
Robert Coupe  
Colonel  
Delaware State Police  
Dover, DE



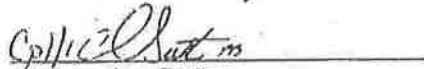
Dennis Schmitt  
Detective



Michael Calloway  
Detective



Fred Chambers  
Detective



Christopher Sutton  
Detective