Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION DOCUMENTS

Section: 40

Federal Bureau of Investigation

[redacted] RMD) (FBI)

From: [redacted] OI) (FBI)
Sent: Thursday, November 30, 2006 3:27 PM
To: [redacted] OI) (FBI)
Subject: FW:

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

-----Original Message-----
From: [redacted] (OI) (FBI)
Sent: Thursday, October 27, 2005 7:38 AM
To: [redacted] (CD) (FBI)
Cc: [redacted] (OTD) (FBI) [redacted] OI) (FBI); [redacted] OI) (FBI) [redacted] (OI) (FBI)
Subject: FW:

~~UNCLASSIFIED~~
NON-RECORD

FYI, for the DCS-3000 (see below)

[redacted] THANKS!)
-----Original Message-----
From: [redacted] OTD) (FBI)
Sent: Monday, October 24, 2005 5:16 PM
To: [redacted] OI) (FBI)
Subject: RE:

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

[redacted]

Regarding the DCS-3000:

(1) a complete description of the types of FISA information stored:
The only information collected and stored by the DCS-3000 is pen-register/trap-trace data. Per CALEA, this information is intercepted by the targets' service providers and delivered to the DCS-3000 in standard formats. The information is parsed based on target telephone number and stored in text-formatted files for each target.

(2) an explanation of how FISA information can be searched and retrieved:
Most field offices use the DCS-3000 as a "front-end" collector. The pen-register/trap-trace information collected by the DCS-3000 is uploaded to the Telephone Application (TA) database at HQ. The FISA pen-register/trap-trace information can be searched using search tools provided by the TA database on FBI Net. The DCS-3000 also has a rudimentary report generation feature and simple text-based search tools for use by technically trained agents and system administrators.

(3) how the FBI's standard minimization procedures are implemented:
The DCS-3000 only collects pen-register/trap-trace information.

DATE: 06-07-2007
CLASSIFIED BY 65179dmh/ksr/maj
REASON: 1.4 (G)
DECLASSIFY ON: 06-07-2032

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

-----Original Message-----
From: [redacted] OI) (FBI)
Sent: Monday, October 24, 2005 2:36 PM
To: [redacted] CD) (FBI)
Cc: [redacted] (OI) (FBI); [redacted] (OI) (FBI); [redacted] OI) (FBI); [redacted] (OI) (FBI); [redacted] NY) (FBI); [redacted] (CD) (FBI); [redacted] (CyD) (CON); [redacted] (OTD) (FBI); [redacted] OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE:

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

All: The FISA Court (FISC) is seeking information about "databases" that contain raw FISA material or U.S. person information from FISA intercepts that is not in indices.

Red Wolf [redacted] can fill in the gaps and correct any misstatements below.)
(1) a complete description of the types of FISA information stored:
[redacted]
(2) an explanation of how FISA information can be searched and retrieved: **Access to FISA audio is generally restricted to the linguists assigned to the case, the supervisor, the case agent, and the system administrator in the office where the audio is collected.** [redacted]
(3) how the FBI's standard minimization procedures are implemented: **Linguists read and sign the court orders certifying that they understand the minimization guidelines specific to each case.**

b2
b6
b7C
b7E

[redacted] answer the questions below.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

DCS-3000: [redacted] can answer the questions about DCS-3000 below.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

(S) [redacted] can answer the questions below.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

b1
b2
b6
b7C
b7E

[redacted] can answer these questions.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

CITA (CITA is still online, but I do not believe any new data has been loaded since EDMS took over the role of Tech Cut Archive. [redacted] should be able to answer the questions below.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

NY Tech Cut Database [redacted] n NY can direct you to someone who can answer the

questions below.)
(1) a complete description of the types of FISA information stored:
(2) an explanation of how FISA information can be searched and retrieved:
(3) how the FBI's standard minimization procedures are implemented:

-----Original Message-----
From [redacted] (CD) (FBI)
Sent: Tuesday, October 18, 2005 2:11 PM
To [redacted] (OI) (FBI)
Subject:

~~UNCLASSIFIED~~
NON-RECORD

Good afternoon,
I attended the EDMS meeting with [redacted] from NSLB last week.

The FISA Court has requested some information on how the FBI is handling FISA information in its various databases. [redacted] asked me to contact you regarding any FBI databases (besides EDMS and DWS) that contain: (1) raw FISA take,or (2) US person information from FBI FISA collection that has not been indexed into general FBI indices. For each of these databases, the Court is asking for: (1) a complete description of the types of FISA information stored, (2) an explanation of how FISA information is handled, specifically the manner in which data can be searched and retrieved, and (3) how the FBI's standard minimization procedures are implemented. (Valerie specifically mentioned CITA and NY's database as examples). Also, are these databases considered to be sub-systems/databases of EDMS? b6 b7C

I appreciate any assistance you can give me. Please let me know if there are other POCs who are better able to answer the questions.

Thanks
[redacted]

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

[redacted] (RMD) (FBI)

From: [redacted] OI) (FBI)
Sent: Thursday, November 30, 2006 3:28 PM
To: [redacted] OI) (FBI)
Subject: FW: FISC database response

~~SECRET~~
RECORD 319 xx

-----Original Message-----
From: [redacted] (OI) (FBI)
Sent: Monday, October 31, 2005 3:10 PM
To: [redacted] (OI) (FBI)
Subject: FW: FISC database response

~~SECRET~~
RECORD 319 xx

Can you give our reply? TKs!
-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, October 31, 2005 2:16 PM
To: [redacted] CyD) (FBI); [redacted] (OI) (FBI); [redacted] OTD) (FBI); [redacted] (CyD) (FBI); THOMAS, MARCUS C. (OTD) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] OGC) (FBI); [redacted] D) (FBI); [redacted] (OGC)(FBI); [redacted] (CD) (FBI); [redacted] OGC) (FBI)
Subject: FISC database response

b6
b7C

~~SECRET~~
RECORD 319 xx

[redacted]

b2
b6
b7C
b7E
b5

[redacted]

b2
b7E

[redacted]

b2
b6
b7C
b7E
b5

[redacted]
Assistant General Counsel
Policy & Training Unit
National Security Law Branch
(202) 324[redacted]

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
SECRET

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
SECRET

Precedence: ROUTINE Date: 10/29/1999

To: Laboratory Attn: Mr. [redacted] QTERF
Mr. [redacted] QTERF (Enc.)
Mr. [redacted] QTERF (Enc.)
Mr. [redacted] QTERF (Enc.)
Mrs. [redacted] QTERF (Enc.)

From: Laboratory
Electronic Surveillance Technology Section/Operational Support Tracking Office
Contact: [redacted] (703) [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] alm

Case ID #: 268-HQ-1217551
268-HQ-1001725

Title: OPERATIONAL SUPPORT TRACKING OFFICE (OSTO)
PROJECT [redacted]
PROJECT REDHOOK
PHASE FIVE REVIEW REPORT

Synopsis: Projects [redacted] and REDHOOK Phase Five Review was held on 10/21/1999 at the Engineering Research Facility. The results, conclusions and recommendations from these reviews are captured in the attached Project [redacted] and Project REDHOOK Phase Five Review Report, dated 10/21/1999.

b2
b6
b7C
b7E

Enclosure(s): Projects [redacted] and REDHOOK Phase Review Report dated 10/21/1999.

Details: The Phase Five Review for Projects [redacted] and REDHOOK was held at the Engineering Research Facility on 10/21/1999. [redacted] Project Leader, Data Intercept Technology Unit, provided an overview and status of current activities for Projects [redacted] and REDHOOK. Key decisions from these presentations are captured within the referenced enclosure.

LEAD(s):

Set Lead 1:

LABORATORY

AT QUANTICO, VA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179dmh/ksr/maj

Precedence: ROUTINE Date: 09/01/1999

To: Laboratory Attn: Mr. [redacted] QT-ERF
Mr. [redacted] QT-ERF
Mrs. [redacted] QT-ERF
(Enclosure)
Mr. Thomas, QT-ERF
Mr. [redacted] QT-ERF
(Enclosure)

b6
b7C

From: Laboratory
Electronic Surveillance Technology Section/EST-4
DITU, QT-ERF
Contact: [redacted] (703) [redacted]

Approved By: [redacted]
Thomas Marcus C

Drafted By: [redacted] llp

Case ID #: 268-HQ-1001725 (Pending)

Title: REDHOOK
PROJECT CLOSEOUT

Synopsis: EST-4 is requesting that the Project Closeout Report for RedHook be approved.

Enclosure(s): Project Closeout Report for RedHook Project

Details: The Laboratory Division, Electronic Surveillance Technology Section, EST-4, is responsible for the development of lawfully authorized digital telephony collection systems. The RedHook Project was developed to facilitate lawfully authorized collection of integrated services digital network (ISDN) traffic on the subscriber's line. The RedHook development effort has been completed. The attached Project Closeout Report documents the results of this effort, and is being submitted for approval.

LEAD(s):

Set Lead 1:

LABORATORY

AT QUANTICO, VA

That ESTS approve the Project Closeout Report for the RedHook ISDN intercept system.

Precedence: ROUTINE
Date: 03/30/1999

To: Finance
Attn: Mr. [redacted] Room 6888
Mr. [redacted] Room 6888
(Enclosure)

Criminal Investigative Laboratory
Mr. [redacted] Room 5155
Mr. [redacted] T ERF
Mr. Thomas, QT ERF
Mr [redacted] QT ERF
(Enclosure)

From: Laboratory
Electronic Surveillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6
b7C

Approved By: [redacted]
Thomas Marcus C

Drafted By: [redacted] llp

Case ID #: (U) 268-HQ-1001725 (Pending)

Title: (U) REDHOOK
CONTRACT ACTION

(C)

Synopsis: ~~(U)~~ [redacted] has delivered funding to the FBI for the production of two integrated services digital network (ISDN) collection systems. The FBI is also funding the purchase of a number of key system components to maximize its present ISDN deployment capability. These pre-production prototypes will be fabricated at Harris Corporation in Melbourne, Florida.

b1
b2
b7E

(U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Enclosure(s): (U) Requisition number 897859

(C)

Details: ~~(U)~~ [redacted] to the FBI for the purchase of two pre-production ISDN intercept systems. These systems will be built by Harris Corporation in Melbourne, Florida.

(U) The DITU will be purchasing a number of system components to maximize the number of lawfully authorized ISDN collections the FBI is able to support. The following is a list of those components DITU will be purchasing; eight line cards to

support processing and distribution units, 18 [redacted] power units, and 18 single slot bridge chassis. The enclosed funding of $130,000 is for the purchase of these components. Residual funding will be used for case support.

b2
b7E

LEAD(s):

Set Lead 1: (Adm)

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

(U) For information only.

Set Lead 2: (Adm)

LABORATORY

AT QUANTICO, VA

(U) For information only.

Set Lead 3: (Adm)

FINANCE

AT WASHINGTON, DC

(C) ~~DE~~ That the Finance Division coordinate the purchase of two pre-production prototypes for [redacted] and system components to support maximizing the FBI's deployment capability.

b1
b2
b7E

Precedence: ROUTINE Date: 08/06/1998

To: Information Resources Attn: Mr. [redacted] QT-ERF

From: Information Resources
Electronic Surveillance Technology Section/CIMU/QT-ERF
Contact: [redacted] (703) [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] ehb

Case ID #: 268-HQ-1001725 (Pending)

Title: RED HOOK
TRIP REPORT

Synopsis: To report the details of Electronics Technician (ET) [redacted] travel to Melbourne, Florida, to attend the Red Hook Digital Intercept System status and planning meeting on 07/29-31/98.

Details: ET [redacted] traveled to Melbourne, Florida to attend a meeting with Harris Company developers which was conducted by Electronics Engineer [redacted] (EST-4). The status of the Red Hook project was discussed. Matters discussed included open tasks, action items, and development time lines. Acceptance testing is tentatively planned for mid September.

A "lunch Box" computer-based Red Hook system, called "Red Hook Lite," was proposed by Harris and approved for development. This system will have a simplified graphical user interface (GUI) and will be designed for quick reaction deployment. ET [redacted] provided input regarding the tactical advantages of the Red Hook Lite system and format of the simplified GUI.

b6
b7C

LEAD (s):

Set Lead 1:

INFORMATION RESOURCES

AT QUANTICO, VA

For information only.

CC: 1 - Mr. [redacted] QT-ERF
1 - Mr. [redacted] QT-ERF

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179DMH/KSR/MAJ

Precedence: ROUTINE Date: 02/05/1998

To: Finance Division Attn: Mr. [redacted] oom 6032
Mr. [redacted] Room 6875
Mr. [redacted] Room 6875
(Enclosure)

National Security Attn: Mr. [redacted] Room 7110
Criminal Investigative Attn: Mr. [redacted], Room 7116
Information Resources Attn: Mr. [redacted] Room 5835
Ms. [redacted] Room 8998

b6
b7C

From: Information Resources
Electronic Surveillance Technology Section, EST-4
NADU, QT ERF
Contact: [redacted] (703) [redacted]

Approved By: [redacted]
Thomas Marcus C
[redacted]

Drafted By: [redacted] llp

Case ID #: 268-HQ-1001725 (Pending)

Title: NETWORK ACCESS DEVELOPMENT UNIT (NADU)
PROJECT REDHOOK
CONTRACT ACTION

Synopsis: The EST-4 Unit is recommending that funding of $650,000 be approved to support the field deployments involving the collection of integrated services digital network (ISDN) and the replacement of eight processing and distribution unit (PDU) systems.

Enclosures: Requisition number 863546

Details: The RedHook ISDN intercept system has successfully completed its development of a personal computer (PC) PDU. The PC PDU is replacing the existing virtual memory extend chassis based solution deployed prior to this development. The EST-4 is requesting that a pre-production quantity of eight PC PDU systems be built to certify production quality and replace systems that are already fielded.

Additionally EST-4 is requesting that a field support task, with the low level development that is involved with field support, be funded through December 1998. The funding required for field support is $300,000. The funding required for the pre-production PC PDUs is $350,000. The total funding required for this contract action is $650,000.

The RedHook system has been successfully deployed in

four locations with additional locations requesting ISDN support. These pre-production PC PDUs will ensure that the FBI maintains a core capability to deploy ISDN intercepts prior to full production quantities being procured.

The field support effort has been extremely valuable in all previous RedHook installations due to the complex nature of both the technologies present in the collection system, the target system, and the forwarding systems.

ISDN is, and will remain, a rapidly developing telecommunications technology. This requires the FBI to maintain a team of engineers capable of developing field modifications to the RedHook system when required to conduct lawfully authorized ISDN collections.

ISDN is typically used in Internet related communications due to its increased speed and reliability over modem communications. These ISDN Internet connections often bring the newest services on-line first adding to the technical overhead on these types of lawfully authorized collections. LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

For informational purposes only.

LEAD (s):

Set Lead 2:

FINANCE DIVISION

AT WASHINGTON, DC

The Finance Division is requested to schedule a Contract Review Board meeting and present the Harris Corporation proposal for RedHook funding.

CC: Mr. Thomas, QT ERF
Mr. [redacted] QT ERF
Mr. [redacted] QT ERF

b6
b7C

Precedence: ROUTINE Date: 07/21/1997

To: Information Resources Attn: Mr. [redacted] Room 5835
(Enclosure)

From: Information Resources
Electronic Surveillance Technology Section, EST-4,
NADU, QT ERF
Contact: [redacted] (703) [redacted]

Approved By: Morris Carolyn G
[redacted]
Thomas Marcus C

b6
b7C

Drafted By: [redacted] llp

Case ID #: 268-HQ-1001725 (Pending)

Title: NETWORK ACCESS DEVELOPMENT UNIT
PROJECT REDHOOK
CONTRACT REVIEW BOARD (CRB) MEETING

Synopsis: This communication is to notify Assistant Director Morris of a CRB meeting on 7/25/97 at 10:00 a.m. to review an enhancement to the RedHook contract with Harris in Melbourne, Florida.

Enclosures: History of contract

Details: The EST-4 Unit has recommended that funding be approved to enhance the RedHook project. This enhancement funding is for development of a new personal computer based processing distribution unit and case support/enhancements to the prototype system.

LEAD (s):

Set Lead 1:

INFORMATION RESOURCES

AT WASHINGTON, DC

For information purposes only.

CC: Mr. [redacted] (Enclosure) QT ERF
Mr. Thomas (Enclosure) QT ERF
Mr. [redacted] (Enclosure) QT ERF

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179DMH/KSR/MAJ

Precedence: ROUTINE Date: 06/30/1997

To: Finance Division Attn: Mr. [redacted] om 6032
Mr. [redacted] Room 6875
Mr. [redacted] Room 6875

(Enclosure) National Security Attn: Mr. [redacted] ROOM 7110
Criminal Investigative Attn: Mr. [redacted] Room 7110
Information Resources Attn: Mr. [redacted] Room 5835
Attn: Ms. [redacted] Room 8998

From: Information Resources
Electronic Surveillance Technology Section, EST-4
NADU, QT ERF
Contact: [redacted] (703) [redacted]

b6
b7C

Approved By: Morris Carolyn G
[redacted]
Thomas Marcus C

Drafted By: [redacted] llp

Case ID #: 268-HQ-1001725 (Pending)

Title: NETWORK ACCESS DEVELOPMENT UNIT (NADU)
PROJECT REDHOOK
CONTRACT ACTION

Synopsis: The EST-4 Unit is recommending that funding of $70,000 be approved to support the Information Resources Division, Investigative Applications Support Unit's Signal Related Information Database Input/Output Format.

b6
b7C

Enclosures: Requisition number 863480

Details: On 6/27/97 [redacted] Unit Chief of the Investigative Applications Support Unit, met with Electronic Surveillance Technology personnel [redacted] and [redacted] to discuss how the RedHook system's collection database output will interface with the Signal Related Information Database Input/Output Format. Also present at the meeting was Tracor employee [redacted]

As a result of this meeting it has become evident that additional funding of $70,000 will be required to characterize the possible output information collected during an ISDN lawfully authorized telecommunication intercept. This funding will be used to purchase and test a majority of the services that ISDN is presently capable of and documenting how those services are stored in the RedHook system's database.

LEAD (s):

Set Lead 1:

FINANCE DIVISION

That the Contract Review Unit coordinate the additional funding to support the Signal Related Information Database Input/Output Format characterization in support of the Investigative Applications Support Unit.

Set Lead 2:

NATIONAL SECURITY

AT WASHINGTON, DC

For information purposes only.

Set Lead 3:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

For information purposes only.

Set Lead 4:

INFORMATION RESOURCES

AT WASHINGTON, DC

For information purposes only.

cc: Mr. [redacted] QT ERF
Mr. Thomas, QT ERF
Mr. [redacted] T ERF
Mr. [redacted] QT ERF

b6
b7C

Precedence: ROUTINE Date: 06/30/1997

Precedence: ROUTINE Date: 05/29/1997

To: Finance Division Attn: Mr. [redacted] oom 6032
Mr. [redacted] Room 6875
Mr. [redacted] Room 6875
(Enclosures 3)
National Security Attn: Mr. [redacted] oom 7110
Criminal Investigative Attn: Mr. [redacted] Room 7116
Information Resources Attn: Mr. [redacted], Room 5835

From: Information Resources
Electronic Surveillance Technology Section, EST-4
NADU, QT [redacted]
Contact: [redacted] (703) [redacted]

b6
b7C

Approved By: Morris Carolyn G
[redacted]
Thomas Marcus C

Drafted By: [redacted] llp

Case ID #: 268-HQ-1001725 (Pending)

Title: NETWORK ACCESS DEVELOPMENT UNIT
PROJECT REDHOOK
CONTRACT ACTION

Synopsis: The EST-4 Unit is recommending that funding be approved to enhance the RedHook processing and distribution unit (PDU). Additional funding is also being asked for to support present and future case support.

Enclosures: STATEMENT OF NEED
INTERNAL CONCEPT PROPOSAL
Requisition # 863473

Details: FBI Contract J-FBI-91-98 was issued to Harris Corporation in 1991. This contract was divided into five phases:

Phase I - Feasibility study,

Phase II - Prove out the study with hardware/software development,

Phase III - Develop a National Law Enforcement Standard,

Phase IV - Build and deliver three prototype Integrated Services Digital Network (ISDN) intercept systems to the FBI for test and evaluation, and

Phase V - Complete a small production run.

At the completion of this contract it was determined that the system required further development prior to implementing Phase V.

FBI Contract J-FBI-95-228 was issued to Harris Corporation in 1995. The purpose of this contract is to ensure that the future RedHook production systems meet the FBI's ISDN intercept requirements. The Contracting Officer's Technical Representative for this contract is Electronics Engineer

b6
b7C

[redacted]

b2
b7E

The RedHook Project is approaching Phase V: the procurement phase. GSA has already given approval for an indefinite purchase - indefinite quantity contract with Harris Corporation with a ceiling of $10,000,000. It is anticipated that this development effort will cost $400,000. The purchase of 11 systems will be the break-even point for the cost of this enhancement.

(S) It is anticipated that there will be multiple United States government agencies purchasing RedHook systems, as well as both the [redacted] b1 b2 b7E

EST-4 is recommending that the Contract Review Unit (CRU) coordinate the tasking of Harris Corporation, Melbourne Government Division to enhance the PDU. Specifically to redesign the VME chassis based system to operate on a Pentium processor based personal computer.

EST-4 is also asking for additional funding for both case support and new development of system enhancements required for future deployments. The additional funding for this effort is $300,000.

Requisition #863393 dated 8/28/96 is in place for $600,000 and requisition #863473 dated 5/29/97 is enclosed to fund this effort. LEAD (s):

Set Lead 1:

FINANCE DIVISION

That the CRU coordinate the enhancement tasks for Harris Corporation to upgrade the RedHook system and add additional funding for case support.

Set Lead 2:

CRIMINAL INVESTIGATIVE

For Information purposes only.

Set Lead 3:

NATIONAL SECURITY

For Information purposes only. b6 b7C

Set Lead 4:

INFORMATION RESOURCES

For Information purposes only.

Mr. [redacted] QT ERF

Mr. Thomas, QT ERF
Mr. [redacted] ERF
Mr. [redacted] T ERF
Mr. [redacted], QT ERF (Enclosures 3)

b6
b7C

Precedence: ROUTINE Date: 01/17/1997

To: Information Resources Attn: Mr.
Mr.
Mr.

From: Information Resource
Electronic Surveillance Technology Section
Network Access Development Unit
Contact: 703

b6
b7C

Approved By:
Thomas Marcus C

Drafted By: llp

Case ID #: 268-HQ-1001725 (Pending)

Title: UNESCORTED ACCESS
ENGINEERING RESEARCH FACILITY (ERF)
NETWORK ACCESS DEVELOPMENT UNIT
ISSUANCE OF RETENTION BADGE

Synopsis: Booz Allen & Hamilton employee is presently assigned to assist the Network Access Development Unit (EST-4) with matters pertaining to EST-4 projects. EST-4 is asking the Technical Operations Section to issue a retention badge to Mr.

b6
b7C

Details: The EST-4 has a number of projects being supported by Booz Allen & Hamilton employee has a Top Secret clearance and presently is allowed unescorted access to the ERF. Because Mr. works in this facility three days a week a retention badge would limit the administrative burden associated with daily checking in.

Mr. has been working for EST-4 for over a year working three days a week on-site. It is expected that Mr. will continue to work at the ERF for a minimum of a year. The point of contact for Mr. is EST-4 Electronics Engineer

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

Issue a retention badge to Mr.

CC: Ms.
Ms.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179DMH/KSR/MAJ

Ms. [redacted]
Ms. [redacted]
Mr. [redacted]
Mr. Thomas
Mr. [redacted]

b6
b7C

Precedence: ROUTINE Date: 01/17/1997

To: Information Resources Attn: Mr. [redacted]
Mr.
Mr.

From: Information Resource
Electronic Surveillance Technology Section
Network Access Development Unit
Contact: [redacted] 703 [redacted]

b6
b7C

Approved By [redacted]
Thomas Marcus C

Drafted By: [redacted] :llp

Case ID #: 268-HQ-1001725 (Pending)

Title: UNESCORTED ACCESS
ENGINEERING RESEARCH FACILITY (ERF)
REDHOOK PROJECT
ISSUANCE OF RETENTION BADGE

Synopsis: Vitro employee [redacted] is presently assigned to assist the Network Access Development Unit (EST-4) with matters pertaining to the RedHook project. EST-4 is asking the Technical Operations Section to issue a retention badge to Mr. [redacted]

b6
b7C

Details: The EST-4 RedHook project is being supported by Vitro employee [redacted] has a Top Secret clearance and presently is allowed unescorted access to the ERF. Because Mr. [redacted] works in this facility five days a week a retention badge would limit the administrative burden associated with daily checking in.

Mr. [redacted] has been working for EST-4 for over a year working five days a week on-site. It is expected that Mr [redacted] will continue to work at the ERF for a minimum of a year. The point of contact for Mr [redacted] is EST-4 Electronics Engineer [redacted]

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

Issue a retention badge to Mr [redacted]

Mrs. [redacted]
Mrs.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179DMH/KSR/MAJ

Mrs. [redacted]
Ms.
Mr.
Mr. Thomas
Mr. [redacted]

b6
b7C

Precedence: ROUTINE Date: 12/03/1996

To: Information Resources

From: Information Resources
Electronic Surveillance Technology Section, EST-4
Contact: [redacted] extension 703[redacted]

Approved By: [redacted]
Thomas Marcus C

Drafted By: [redacted] :llp

Case ID #: (U) 268-HQ-1001725 (Pending)

Title: (U) EST-4
REDHOOK
TRIP REPORT

(U)

Synopsis: ~~(S)~~ EST-4 Electronics Engineer (EE) [redacted] traveled to the San Francisco Office (SFO) to survey a possible FCI deployment of the RedHook integrated services digital network (ISDN) intercept system at [redacted]

(U) ~~Classified By: G-3~~
~~Declassify On: X-1~~

(U) Details: ~~(S)~~ On 11/13/96 EE [redacted] traveled to the SFO to conduct a site survey for a possible FCI deployment of the RedHook ISDN intercept system. The technical point of contact in the SFO for this effort is Special Agent (SA) [redacted] The case agent is SA [redacted] also from the SFO.

(U) ~~(S)~~ The under cover (UC) location for the collection and storage of the data forwarded from the RedHook collection device is in [redacted] California. This site has existing T1 facilities but this equipment does not support the B8ZS encoding required to forward the intercepted data being forwarded from the subscriber location.

(U) ~~(S)~~ To ensure that the facilities are correctly configured to support this ISDN intercept, a T1 connection is being engineered by [redacted] from the [redacted] location to the UC site in [redacted] This requires that the SFO purchase two D-4 channel banks configured to support B8ZS line encoding. SA [redacted] is coordinating this effort with [redacted] from Lucent Technologies.

(U) ~~(S)~~ SA [redacted] made a special request that the RedHook system be configured to operate with a Revox reel-to-reel tape recorder for this mission. This will facilitate the

b2
b6
b7C
b7E

translators operation at the SFO. EE [redacted] is testing this configuration in the EST-4 laboratory to ensure that this configuration operates properly.

(C) ~~(S)~~ At [redacted] SA [redacted] introduced EE [redacted] to [redacted] from [redacted] Security. SA [redacted] EE [redacted] and Mr. [redacted] visited the [redacted] site where access to the subscriber's ISDN line is available. The subscriber is being serviced from a 5ESS switch configured to deliver a four-wire interface direct to the customer. The RedHook system is designed to only intercept at the two-wire interface. The [redacted] switch manager will convert the subscriber's line from four-wire to two-wire prior to the deployment of the RedHook system. The switch manager will then convert the line back to a four-wire interface prior to the service reaching the subscriber's desktop.

(U) ~~(S)~~ The [redacted] switch manager will have to find a way to deploy a network termination type 1 (NT1) device into the subscriber's facility without alerting other telephone maintenance personnel. The switch manager will contact EE [redacted] or SA [redacted] if he encounters any difficulty implementing this NT1 deployment.

(U) ~~(S)~~ The location of the intercept equipment is in a room with a combination spin lock. This room is in a separate building from the subscriber. The room that will house the bridge unit and power supply has a 19-inch rack and an uninterruptable 110 AC power supply available to support this installation. The patch panel was identified that will connect the ordered T1 line to the UC site.

(U) ~~(S)~~ The target installation date for this RedHook system is after 12/15/96. A RedHook fly-away system has been identified and is being checked out to support this installation.

LEAD (s):

Set Lead 1:

INFORMATION RESOURCES

For information only purposes.

CC: Mr [redacted]
Mr. Thomas
Mr. [redacted]
Mr.
Mr.
Mr.

b2
b6
b7C
b7E

b6
b7C

Precedence: ROUTINE Date: 07/1/1996

To: Information Resources Attn: Mr. [redacted]

From: Information Resources
Electronic Surveillance Technology Section, EST-4
Contact: [redacted] extension (703) [redacted]

Approved By: [redacted]
Thomas Marcus C

Drafted By: [redacted] llp

Case ID #: (U) 269-HQ-1001725 (Pending)

Title: ~~(C)~~ NETWORKS ACCESS DEVELOPMENT (EST-4)
REDHOOK PROJECT
(C) [redacted]

Synopsis: ~~(C)~~ Trip report for travel to [redacted] in direct support of loaned RedHook equipment [redacted]

(U) ~~Derived from: G-3~~
~~Declassify On: X-1~~

(C) Reference: (U) FD540 #1612992 Serial

Details: ~~(C)~~ On 6/4/96 Supervisory Special Agent [redacted] and Electronics Engineer (EE) [redacted] traveled to [redacted] at the request of [redacted]

(C) ~~(C)~~ The purpose of this travel was to demonstrate a RedHook integrated services digital network (ISDN) intercept system for possible deployment and purchase of additional systems by [redacted]. The RedHook system that was used for this demonstration is on a temporary loan to [redacted] for three months with an anticipated return date of 9/6/96.

(C) ~~(C)~~ The system was successfully installed and tested at the [redacted] facility. During testing it was discovered that the ISDN lines installed for this demonstration were not functioning normally. The lines were experiencing abnormally high far end bit errors (FEBEs). These FEBEs were occurring in bursts that repeatedly caused the RedHook serial bridge to go into a safety

bypass mode. When an ISDN line tester was placed on the line, the FEBEs were found to be intermittent and of varying severity.

(C) ~~DEK~~ The [redacted] were briefed on the RedHook system during a period when the FEBEs were not as severe. Following the briefing, EE [redacted] gave a live demonstration using the ISDN lines that were experiencing FEBEs. During the demonstration, the system performed perfectly.

(C) ~~DEK~~ After the briefing was concluded, the ISDN lines again returned to a state of abnormally high FEBEs. [redacted] RedHook system to another location that has known good lines.

(C) ~~DEK~~ After returning to the Engineering Research Facility, the [redacted] personnel have repeatedly encountered the FEBEs and asked if the RedHook system could be modified to operate in this abnormal environment. EE [redacted] has briefed them on the fact that the system presently allows 250 times the bit error rate allowed by the Comite Consultatif International de Telegraphique et Telephonique (CCITT) standards for ISDN lines. EE [redacted] explained that it is not feasible to further relax the RedHook bit error safety bypass function. This would inevitably be responsible for a subscriber, on a lawfully authorized intercept, sending a repair person from the telephone company out to repair a RedHook serial bridge under these worst case conditions.

b1
b2
b6
b7C
b7E

(C) ~~DEK~~ EE [redacted] again advised [redacted] that the best possible action, at this time, is to transport the system to another location that has known good lines and proceed with the testing of the RedHook system.

CC: Mr. Thomas
Mr. [redacted]
Mr.

5/28/96

X

X

FM FBI QUANTICO (268-HQ-1001725)/ROUTINE/

TO DIRECTOR FBI (268-HQ-1001725)/ROUTINE/

[redacted]/ROUTINE/

BT

S E C R E T (S)

CITE: //0857//

PASS: FBIHQ, INFORMATION RESOURCES DIVISION, MRS. MORRIS, ROOM 5829.

(U) SUBJECT: TRAVEL TO [redacted] 5/30/96 AND 6/4-7/96. (U)

FOR THE INFORMATION OF [redacted] EST-4, ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION, INFORMATION RESOURCES DIVISION, FBIHQ, HAS BEEN OFFICIALLY REQUESTED [redacted] TO PROVIDE TECHNICAL ASSISTANCE WITH THE INITIAL SETUP OF AN EXPERIMENTAL SYSTEM. THIS SYSTEM, CODENAMED REDHOOK, IS AN INTEGRATED SERVICES DIGITAL NETWORK INTERCEPT SYSTEM. FBI PERSONNEL ARE REQUESTED TO DELIVER AND SETUP ONE SYSTEM FOR [redacted] LS TO RETURN THE SYSTEM AFTER THREE MONTHS. (U)

(U) IN ATTENDANCE FROM EST-4 WILL BE SUPERVISORY SPECIAL AGENTS [redacted] ELECTRONICS ENGINEER [redacted] AND ELECTRONICS TECHNICIAN [redacted] (U)

(S) TRAVEL ON 5/30/96 WILL BE A ROUND TRIP ON A BUREAU PLANE WITH THE SOLE PURPOSE OF DELIVERING THE REDHOOK SYSTEM TO [redacted]

TRAVEL ON 6/4-7/96 WILL BE BY COMMERCIAL AIRLINE. DURING THESE DATES, THE ABOVE MENTIONED PERSONNEL WILL ASSIST [redacted] IN (S) THE SETUP AND EVALUATION OF THE REDHOOK SYSTEM. [redacted] ASSISTANCE IS REQUIRED FOR LODGING. A RENTAL CAR IS REQUIRED FOR THE DURATION OF THE STAY.

POINT OF CONTACT FOR THIS EFFORT IS [redacted] MR. [redacted] CAN BE REACHED AT 703 [redacted]

CLASSIFIED BY: G-3, X-1.

BT COPY COUNT PAGE
268-HQ-1001725

b1
b2
b6
b7C
b7E

Case ID : 268-HQ-1001725 Serial : 54

~~SECRET~~

MR. [redacted]
MR. THOMAS
MR. [redacted]
MR.
MR.
MR.
MR.

b6
b7C

JLE/LLP (8)

Precedence: ROUTINE Date: 4/22/1996

To: Information Resources Attn: [redacted] (Enclosure)

From: Information Resources
Electronic Surveillance Technology Section, EST-4
Contact: [redacted] extension 703 [redacted]

Approved By: [redacted]
Thomas Marcus C

Drafted By: [redacted] :llp

Case ID #: 269-HQ-1001725 (Pending)

Title: NETWORKS ACCESS DEVELOPMENT (EST-4)
REDHOOK PROJECT
TRIP REPORT 4/10/96 (U)

Synopsis: Trip report to Harris at Melbourne, Florida to support project RedHook. (U)

Classification: ~~CONFIDENTIAL~~

Enclosure: Monthly Status Report on RedHook Engineering Services Program for April 1996. (U)

(U) Details: The RedHook project is an integrated services digital network (ISDN) intercept system. It is designed to capture ISDN signals between the telephone company central office and the subscriber's residence. The RedHook system inserts a bridging device into the "U" interface and forwards both the subscriber's and associate's signal to its distribution and minimization components. ~~(C)~~

Case ID : 268-HQ-1001725 Serial : 52

On 4/10/96 Electronics Engineer (EE) [redacted] of the EST-4, met with Harris personnel at their Melbourne, Florida location to review progress on the RedHook project and give an award fee presentation. Systems Engineer [redacted] represented [redacted] and EE [redacted] represented the [redacted] Attending from Harris were [redacted] from Vitro Corporation, represented EST-4 as a contract advisor. (U)

The new multi-point task, which will allow the system to discriminate between multiple telephone numbers sharing a single wire pair, is significantly ahead of schedule and well under cost. The software coding required to perform this task was lessened due to good coding practice on the original design. The system will now have a menu pick in the set-up menu to select any combination of available telephone numbers. The formal acceptance test plan (ATP) for this task is scheduled for late May. (U)

Work on the personal computer (PC) workstation is starting and the Harris team has identified a pentium based [redacted] platform to test. This system will use SUN Microsystems' [redacted] If this software allows the RedHook software to [redacted] this could significantly reduce maintenance costs for the RedHook system. (U)

Task 2, the addition of National ISDN 1 (NI-1) and Northern Telecom (NT) Custom, has gone through an internal design review and is ready to begin coding software. This task is considerably ahead of schedule. Again this is due in large part to the good coding practice implemented by the Harris team on the original design. (U)

Upgrades to the operating systems on both the workstation software and the process and distribution unit (PDU) were performed successfully. The PDU upgrade involved significant trouble shooting on the part of Harris. The sources of the difficulties were identified at the software design house

that maintains the commercial software. (U)

Task 1: workstation anomalies, has been completed with all identified anomalies corrected. Task 1 will resume after the ATP is completed and any additional anomalies are identified during testing. (U)

A commercial source, Melcher, has been identified for a rack mounted power supply. This replacement power supply will replace the fully custom Harris developed and Harris manufactured rack mounted power supply. The Melcher supply was released for sale after the design and manufacture of the Harris custom supply. The Melcher supply is manufactured by a Swiss company for commercial telephone company use and meets or exceeds all FCC requirements for installation in a telephone company central office. (U)

(U)

The bridge units have been upgraded to include the ability to stay logically linked to the central office when the subscriber powers down their network terminator 1 (NT1). This problem arises when a terminal adapter is either powered from the same source as a computer or is internal to the computer and the system is powered down. The bridge sensed this as a fault condition and went into a bypass mode. The system now maintains the central office link and swaps status bits to remain transparent from the network side of the bridge. (U)

(U) At the subscriber's side the bridge sends signals to the NT-1 waiting for it to be powered on. When it is powered on the time required for the NT-1 to power up and synchronize with the network is identical to the time required without the bridge present. This change required a change in code used in the programmable read only memory (PROM). (U)

A retrofit of existing bridges is being done on both the card based serial bridges and the field operable serial bridges. The field operable serial bridge retrofit requires that the old PROMs be floated off the surface mount boards and new parts be installed. These bridges have had a lot of rework performed on them in the past so there is a possibility that one

or two field operable bridge units may not survive this procedure. (U)

While the retrofit of the PROMs is taking place, two field operable serial bridge units will be outfitted with new low power AT&T ISDN transceivers. This should increase the distance from which the field operable serial bridge can be remotely powered. The increase in distance will have to be determined when the bridges are recertified after the parts placements are complete. (U)

The ATPs for the bridges, PDU, and workstation are scheduled for late May. EE [redacted] and Vitro employee [redacted] will be present for the testing. EST-4 will invite an EST-3 representative to be present. (U)

The Harris award fee for this four month evaluation period was 85 percent of the award fee in excess of the minimum. This was achieved by scoring 94 out of a possible 100 points on the evaluation criteria. This Harris team is performing extremely well by meeting or exceeding target development dates and coming in under budget for the major tasks worked on. (U)

WORK COPY ROUTING SHEET

CC: Mr. [redacted]
(Attn: Mr. [redacted] (Enclosure)
Mr. Thomas (Enclosure)
Mr. [redacted]
(Attn: Mr. [redacted] (Enclosure)
Mr [redacted] (Enclosure)

CONFIDENTIAL

Mr. [redacted] (Enclosure)

b6
b7C

~~CONFIDENTIAL~~

IT STRAT PLAN CATEGORY	FBI LOB	OTD collection system and information	Division	Line Item Name (Investment / Project / IT Asset)	Acronym	Investment Description (limited to 255 characters)	EX53	CY 06	BME 07($M) BY	SS 07 ($M) BY	EX300	OME (07)	SS (07)	OME (08)	SS (08)	FBI Projects	FY05 ($M)	FY06 ($M)	FY07 ($M)	MITSL
	ELSUR	✓ Includes DCS3000, DOS5000, DCS6000	OTD	Digital Collection System - IT Interface	DCS-IT	The Digital Collection Project ensures the ability of the FBI to collect evidence and intelligence to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. This project includes upgrades to the DCS 3000, DCS 5000, and DCS 6000 National Security Collection Systems.	X	$35.775	$32.688	$6.502	X	$32.688	$6.502	$ 17.925	$6.500	X	$28.000	$34.368		X

OTHER outside the scope

pg-1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179dmh/ksr/maj

IT STRAT PLAN CATEGORY	FBI LOB	OTD Collection and Information System	Division	Line Item Name (Investment / Project / IT Asset)	Acronym	Investment Description (limited to 255 characters)	EX53	CY 06	DME 07($M) BY	SS 07 ($M) BY	EX300	DME (07)	SS (07)	DME (08)	SS (08)	FBI Projects	FY05 ($M)	FY06 ($M)	FY07 ($M)	NITSL
sys	ELSUR	✓	OTD	Digital Collection System 3000 - IT Interface	DCS 3000-IT	assist law enforcement agencies (LEAs) with collecting and processing data for court-ordered electronic surveillance (ELSUR) operations. LEAs dial into switches.														X
net	ELSUR	✓	OTD	Digital Collection System Network	DCSNet	The Digital Collection Systems Network (DCSNET) is a transport mechanism for moving CALEA CDC and streamed CCC data from the service provider sources to the proper FBI Field Office destinations. DCSNET is used entirely for collection of evidence and is not connected to FBI IT networks or systems.		$0.000	$0.000	$0.000		$ -	$ -	$ -	$0.000		$0.000	$0.000	0	X

pg-2

OTHER outside the scope

OTD / Collection Architecture Meeting – March 17, 2006
Summary Notes / Action Items

Workshop discussion points

- Need to include common EA terms in the read-ahead materials. OTD is especially interested in definitions for Information Technology (IT) and National Security System.
  - A significant portion of OTD's mission systems are clandestine technologies (ClanTech) and are not considered IT and do not touch the FBI enterprise. The focus of the FBI EA program should be on those OTD systems that interface with the FBI IT environment.
  - Collection assets produce intelligence and do not produce records.
- Need to add satellites to the list of OTD priority projects (Technical Response Unit (TRU) Communication System).
- Need to better define the OTD budget line items so that our reports do not over-inflate FBI IT budget totals.
- OTD needs OCIO help with EDMS and the current service level agreements (SLA). Recent system outages have impacted mission accomplishment.

Business Architecture

- EDMS should be mapped to the BRM Intelligence Collection sub-function (recommended update for the next OMB Exhibit 300 submission).
- OTD is initiating a Division-level Transition/Consolidation Plan to move towards a Consolidated FISA System in the future.

Services and Capabilities

- OTD has service needs for storage, search, evidence handling, and digital media.
  - Currently they store/back-up both FISA and criminal content on removable media.
  - OTD identified an evidence handling dependency with LD's Laboratory Information Management System (LIMS).

b2
b7E

T&S Findings and Recommendations

- Need to compare OTD initiatives
  - See the Emerging Technology Bulletin Research Bulletin at [redacted] examples that discuss wireless technologies and many other topics and their impacts to law enforcement and collection.

Action Items

- Follow-up with [redacted] for edits to the FBI Traceability Matrix.
  - DCS is the common name for DCS 3000, 5000, and 6000 (DCS redundant).
  - DCS 5000 is synonymous with [redacted] redundant).
  - LEEDS is not an OTD system (determine the sponsor).
- Follow-up with [redacted] for the OTD Transition Plan (Consolidated FISA System).
- [redacted] plans to visit OTD to gain a better understanding of where OTD systems interface with the FBI enterprise for inclusion in the FBI T&S Plan.
- Follow-up with OTD on the status of the E-Requisition initiative.
- Follow-up with OTD on the break out of their IT budget line items vs Collections budget items.

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179dmh/ksr/maj

Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION DOCUMENTS

Section: 41

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 7
Page 2 ~ b2, b5, b6, b7C, b7E
Page 3 ~ b2, b5, b6, b7C, b7E
Page 4 ~ b2, b5, b6, b7C, b7E
Page 5 ~ b5
Page 77 ~ b5, b6, b7C
Page 78 ~ b5, b6, b7C
Page 79 ~ b5, b6, b7C

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

~~SECRET~~

OVERVIEW OF DCS SYSTEMS FOR [redacted] DOC

16 JULY 2003

Collection Systems

b6
b7C

DCS 3000 and DCS 6000 are unclassified systems and each is type accredited as a standalone system.

[redacted]/DCS5000 are classified systems that are not accredited but are in the process. However, there are significant unresolved issues. (We are identifying the significance of the identified risks to determine what plan of action to take to resolve issues.) It is highly unlikely that the C&A of these systems will be complete before October 2003.

b2
b7E

DCSNet will be a single network that will permit field offices to connect to telcos via a single network. The contract has not yet been awarded for this system and there is no current C&A activity.

The DCS 3000 will the interface between the DCSNet, and the DCS 6000 and [redacted] DCS 5000.

Consideration has been given to re-accrediting the DCS 3000 to document its role as the system in the middle between the DCSNet and the DCS 6000 and the [redacted] DCS 5000.

The interface between DCS 3000 and DCS 6000 is a firewall (We need to determine how to handle this interface from a C&A perspective. ISA is inappropriate and MOA/MOU do not seam to be appropriate. Perhaps an ICD, firewall policy or a connection approval process should be created.)

b2
b6
b7C
b7E

Interface between DCS 3000 and [redacted] DCS 5000 is the CI 100, which is being C&Aed separately.

We understand tha[redacted] will or has become the SCO for all of these systems.

We are scheduled to meet with ERF staff at 1000, on Tuesday 29 July 2003 at ERF office at Quantico.

FBI Digital Collection

Exhibit 300: Part I: Summary Information and Justification (All Capital Assets)

I.A. Overview

1. Date of Submission:	8/4/2006
2. Agency:	Department of Justice
3. Bureau:	Federal Bureau of Investigation
4. Name of this Capital Asset:	FBI Digital Collection
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	011-10-01-02-01-2503-00
6. What kind of investment will this be in FY2008? (Please NOTE: Investments moving to O&M ONLY in FY2008, with Planning/Acquisition activities prior to FY2008 should not select O&M. These investments should indicate their current status.)	Mixed Life Cycle
7. What was the first budget year this investment was submitted to OMB?	FY2001 or earlier

8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap:

Digital Collection consists of the DCS-3000, DCS-5000, and DCS-6000, which provide digital collection tools, foreign counterintelligence gathering, and law enforcement evidence collection, respectively. Today's information technology capabilities afford terrorists and criminals many avenues to coordinate and commit offenses against US citizens and interests. Traditional phones were the primary avenue criminals used to communicate information regarding unlawful acts. Today, more incidents are committed and facilitated by terrorists using high-tech, non traditional communications methods. Communications methods are dramatically increasing in number and complexities, resulting in the continual and evolving need for advanced methods of electronic surveillance of voice communications - methods of electronic surveillance have limited-life utility in intercepting newer, more secure types of publicly offered communications. The expansion of electronic surveillance activity in frequency, sophistication, and linguistic needs continues to increase the level of support required. An important factor behind this expansion is the changing demographic of targets that must be monitored by investigators. The FBI must supply equipment and analytical tools to uniquely qualified language specialists to speed the translation and transcription process to meet the investigators' needs. Further, the life span of today's technology is often much shorter than older technologies, resulting in more frequent need for solution development. Terrorist and criminal activity has expanded across international boundaries. Current United States-based intercept technologies and collection capabilities are not always sufficient to meet global requirements. Increased coordination and cooperation with other Government agencies and Governments of other countries place are needed. Digital collection must continue to clearly define electronic surveillance requirements and closely track manufacturers' approaches and solutions. Collection equipment manufacturers continue toward complying with technical standards as a result of the Communications Assistance to Law Enforcement Act (CALEA). One result of the CALEA standard is more information is available for collection. This increase in data coupled with the increased complexity of computer-based electronic surveillance information management systems will impose a requirement for efficient distribution to users and their respective collection systems

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this	5/19/2006

approval?	
10. Did the Project Manager review this Exhibit?	Yes
11. Contact information of Project Manager?	
Name	[redacted]
Phone Number	703-[redacted]
Email	[redacted]
12. Has the agency developed and/or promoted cost effective, energy efficient and environmentally sustainable techniques or practices for this project.	Yes
a. Will this investment include electronic assets (including computers)?	Yes
b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only)	No
1. If "yes," is an ESPC or UESC being used to help fund this investment?	No
2. If "yes," will this investment meet sustainable design principles?	No
3. If "yes," is it designed to be 30% more energy efficient than relevant code?	
13. Does this investment support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Human Capital, Expanded E-Government
13a. Briefly describe how this asset directly supports the identified initiative(s)?	Strategic Management of Human Capital. The FBI acquires individuals with rare linguistic skills by collocating and networking the collection assets within proximity for employment, training, and development. A work flow management module is used by operations managers monitor productivity and distribute work accordingly. Expanded E-Gov. Systems are used in internal and external collaboration with Joint Tactical Task Forces, other federal departments, and intelligence organizations.
14. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.)	No
a. If "yes," does this investment address a weakness found during the PART review?	No
b. If "yes," what is the name of the PART program assessed by OMB's Program Assessment Rating Tool?	
c. If "yes," what PART rating did it receive?	
15. Is this investment for information	Yes

b6
b7C

technology?

If the answer to Question: "Is this investment for information technology?" was "Yes," complete this sub-section. If the answer is "No," do not answer this sub-section.

For information technology investments only:

16. What is the level of the IT Project? (per CIO Council PM Guidance)	Level 1
17. What project management qualifications does the Project Manager have? (per CIO Council PM Guidance):	(4) Project manager assigned but qualification status review has not yet started
18. Is this investment identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's "high risk" memo)?	No
19. Is this a financial management system?	No
a. If "yes," does this investment address a FFMIA compliance area?	No
1. If "yes," which compliance area:	
2. If "no," what does it address?	

b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52

20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)

Hardware	33
Software	3
Services	38
Other	26

21. If this project produces information *dissemination products* for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities?	N/A

22. Contact information of individual responsible for privacy related questions:

Name	[redacted]
Phone Number	202-32[redacted]
Title	[redacted]
E-mail	[redacted]

b6
b7C

23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?	No

I.B. Summary of Funding

Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be excluded from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The total estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

Table 1: SUMMARY OF SPENDING FOR PROJECT PHASES
(REPORTED IN MILLIONS)
(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)

	PY - 1 and Earlier	PY 2006	CY 2007	BY 2008	BY + 1 2009	BY + 2 2010	BY + 3 2011	BY + 4 and Beyond	Total
Planning									
Budgetary Resources	11.075	0	2.554	2.554	0	0	0	0	16.183
Acquisition									
Budgetary Resources	136.339	0	0	17.359	16.261	0	0	0	169.959
Subtotal Planning & Acquisition									
Budgetary Resources	147.414	0	2.554	19.913	16.261	0	0	0	186.142
Operations & Maintenance									
Budgetary Resources	52.735	28.124	35.446	15.547	17.075	49.526	44.026	44.125	286.604
TOTAL									
Budgetary Resources	200.149	28.124	38	35.46	33.336	49.526	44.026	44.125	472.746
Government FTE Costs									
Budgetary Resources	7.14	1.905	1.905	14.263	14.263	14.263	14.263	14.263	82.265
Number of FTE represented by Costs:	7	7	7	21	21	21	21	21	126

Note: For the cross-agency investments, this table should include all funding (both managing partner and partner agencies). Government FTE Costs should not be included as part of the TOTAL represented.

2. Will this project require the agency to hire additional FTE's? Yes

a. If "yes," How many and in what year? *Beginning in FY08 ten Electronic Techs* are requested to perform requirements generation, testing/evaluation, installation of new/upgraded equipment, and user training as well as, system administration expertise, telephonic/on-site technical support and system maintenance support for over 1,300 users. Four Electronic Engineers are required to provide technical expertise related to electrical interactions within internal system components and external telecom service provider components/equipment.

3. If the summary of spending has changed from the FY2007 President's budget request, briefly explain those changes:

The FBI is in the process of analyzing alternatives for the next phase in FISA (What is this? Acronyms used the first time must be spelled out) collection systems. The requested personnel enhancement of 14 personnel and non-personnel enhancement of $11,035,000 will enhance the Digital Collection project's capacity to provide next generation systems, facilities, and capabilities to enable continuance of audio and

data collection in the furtherance of the FBI's FCI and Counterterrorism (CT) responsibilities, seamless transition to regionalized collection, and provide replacement equipment which will be required for inoperable systems and component replacements which be required for obsolete equipment. Systems are nearing the end of their life cycle and require substantial investment in maintenance costs to maintain an adequate technological capability until they are replaced. Major overhaul or replacement of these systems will become a necessity beyond FY 2007. The deployment of advanced digital collection systems, which meet the FCI digital collection' regional architecture represents a significant and critical factor in collection implementation. This requires additional knowledgeable staff for installation, training, and maintenance as well as provision of a new generation of collection systems to collect information in the most efficient manner. Contractor support, currently performing these functions, will not be available in FY08. The nonpersonnel enhancement will be used for new systems and equipment purchases ($6,850,000); system upgrades and installation ($685,000); and service maintenance agreements ($3,500,000). Collection systems will be required to interface with the upcoming Electronic Surveillance Database Management System (EDMS) to maintain current capabilities until their replacement. Without the requested resources, the number of funded contractor positions is expected to increase.

I.C. Acquisition/Contract Strategy

1. Complete the table for all (including all non-Federal) contracts and/or task orders currently in place or planned for this investment. Total Value should include all option years for each contract. Contracts and/or task orders completed do not need to be included.

b6
b7C

Contracts/Task Orders Table:

e :t d?	If so what is the date of the award? If not, what is the planned award date?	Start date of Contract/ Task Order	End date of Contract/ Task Order	Total Value of Contract/ Task Order	Is this an Interagency Acquisition?	Is it performance based?	Competitively awarded?	What, if any, alternative financing option is being used?	Is EVM in the contract?	Does the contract include the required security and privacy clauses?	Name of CO	CO Contact infor (phone/ema
	8/1/2005	8/1/2005	4/30/2010	12.1	No	No	Yes	NA	No	Yes		
	9/29/2002	9/29/2002	9/28/2008	14	No	No	Yes	NA	No	Yes		
	4/1/2005	4/1/2005	7/1/2006	1.097	No	No	Yes	NA	No	Yes		
	9/15/2003	9/15/2003	9/15/2008	47	No	No	Yes	NA	No	Yes		
	9/3/2003	9/3/2003	9/8/2008	1.091	No	No	Yes	NA	No	Yes		
	10/1/2003	10/1/2003	9/30/2008	9	Yes	No	Yes	NA	No	Yes		
	10/7/2004	10/7/2004	10/5/2009	1.091	No	No	Yes	NA	No	Yes		

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:

Contracts supporting Digital Collection are legacy contracts awarded prior to EVMS requirements. (EVMS has been a requirement since the inception of the Clinger-Cohen Act). However, current risks for contract performance rests with the firm fixed price contractors. Technical, scheduling, and cost performance is

managed by the Digital Collection project.

3. Do the contracts ensure Section 508 compliance?	Yes
a. Explain why:	Contracts supporting this requirement ensure Section 508 compliance in order to meet legal requirements as well as satisfy needs of user personnel.
4. Is there an acquisition plan which has been approved in accordance with agency requirements?	Yes
a. If "yes," what is the date?	10/29/2000
b. If "no," will an acquisition plan be developed?	
1. If "no," briefly explain why:	

I.D. Performance Information

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency (e.g., improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative or qualitative measure.

Agencies must use Table 1 below for reporting performance goals and measures for all non-IT investments and for existing IT investments that were initiated prior to FY 2005. The table can be extended to include measures for years beyond FY 2006.

Performance Information Table 1:

Fiscal Year	Strategic Goal(s) Supported	Performance Measure	Actual/baseline (from Previous Year)	Planned Performance Metric (Target)	Performance Metric Results (Actual)
2000	Protect America against the threat of terrorism	Number of standard Title 50 digital collection systems in field offices	90% of Title 50 systems collect via analog inputs	Increase digital collection systems by 10%	Increased digital collection systems by 10%
2000	Enforce federal criminal laws	Near end of life Title III systems deployed in field offices	95% of Title II systems end of life	Deploy additional 10% of Title III systems	Deployed additional 30% of Title III systems
2001	Identify, prevent and defeat foreign intelligence operations	Number of standard Title 50 digital collection systems in field offices	80% of Title 50 systems collect via analog inputs	Increase digital collection systems by 40%	Increased digital collection systems by 50%
2001	Prevent terrorist acts and protect critical	Lines of input supported for Title III and Title 50	Total lines of input for analog and digital collection	Increase lines of digital collection input by 100%	Increased lines of digital collection input by 98%

	infrastructure	digital collection	(# classified)		
2001	Enforce federal criminal laws	Near end of life Title III systems deployed in field offices	65% of Title II systems end of life	Deploy additional 10% of Title III systems	Deployed additional 20% of Title III systems
2002	Identify, prevent and defeat foreign intelligence operations	Number of standard Title 50 digital collection systems in field offices	30% of Title 50 systems collect via analog inputs	Increase digital collection systems by 10%	Increased digital collection systems by 10%
2002	Prevent terrorist acts and protect critical infrastructure	Lines of input supported for Title III and Title 50 digital collection	Total lines of input for analog and digital collection (# classified)	Increase lines of digital collection input by 30%	Increased lines of digital collection input by 16%
2002	Enforce federal criminal laws	Near end of life Title III systems deployed in field offices	45% of Title II systems end of life	Deploy additional 30% of Title III systems	Deployed additional 40% of Title III systems
2003	Identify, prevent and defeat foreign intelligence operations	Number of standard Title 50 digital collection systems in field offices	20% of Title 50 systems collect via analog inputs	Increase digital collection systems by 20%	Increased digital collection systems by 20%
2003	Prevent terrorist acts and protect critical infrastructure	Lines of input supported for Title III and Title 50 digital collection	Total lines of input for analog and digital collection (# classified)	Increase lines of digital collection input by 300%	Increased lines of digital collection input by 346%
2003	Enforce federal criminal laws	Near end of life Title III systems deployed in field offices	5% of Title II systems end of life	Deploy additional 5% of Title III systems	Deployed additional 5% of Title III systems
2004	Identify, prevent and defeat intelligence operations conducted by foreign power	Lines of input supported for Title III and Title 50 digital collection	Total lines of input for analog and digital collection (# classified)	Increase lines of digital collection input by130%	Increased lines of digital collection input by 135%
2004	Prevent, disrupt and defeat terrorist operations before they occur	System information storage capacity for collected intelligence	Total storage capacity 12,500GB	Increase system storage capacity by 9%	Increased system storage capacity by 12%
2004	Identify, disrupt and dismantle targeted international drug trafficking organizations	System information storage capacity for collected evidence	Total storage capacity 4,200GB	Increase system storage capacity by 9%	Increased system storage capacity by 12%
2005	Prevent, disrupt, and defeat terrorist operations before they occur	System capacity available to translate and transcribe intercepted Title 50 information	680 linguists and agents supported	Increase capacity for users supported by 37%	Increased capacity for users supported by 37%
2005	Prevent Terrorism and Promote the Nation¿s Security	Lines of input supported for Title III and Title 50 digital collection	Total lines of input for analog and digital collection (# classified)	Increase lines of digital collection input by 110%	Increased lines of digital collection input by 109%
2005	Enforce Federal Laws and represent the Rights and Interests of the	Lines of input supported for Title III digital collection	Total lines of input for digital collection (# classified)	Increase lines of digital collection input by 30%	Increased lines of digital collection input by 60%

	American People				
2006	Prevent Terrorism and Promote the Nationís Security	Collected information meets applicable security standards and policies	Title 50 system certification and accreditation incomplete	Certify and accredit Title 50 system	Title 50 system certified and accredited
2006	Prevent, disrupt, and defeat terrorist operations before they occur	Lines of input supported for Title 50 digital collection	Total lines of input for digital collection (# classified)	Increase lines of digital collection input by 10%	Increased lines of digital collection input by 4%
2006	Enforce Federal Laws and represent the Rights and Interests of the American People	Lines of input supported for Title III digital collection	Total lines of input for digital collection (# classified)	Increase lines of digital collection input by 9%	Increased lines of digital collection input by 8%
2007	Effectively utilize applied science and engineering resources to empower the FBIís investigative and intelligence operations and thwart the techniques of our adversaries	Automated voice to text tools available (language translation)	No automated voice to text tools available	Implement initial capability for voice to text tools	
2007	Effectively utilize applied science and engineering resources to empower the FBIís investigative and intelligence operations and thwart the techniques of our adversaries	Voice recognition tools available for Title 50 system	No voice recognition tools available for Title 50 systems Implement initial capability for voice to text tools	Implement initial capability for voice to text tools	
2007	Effectively utilize applied science and engineering resources to empower the FBIís investigative and intelligence operations and thwart the techniques of our adversaries	Improve speed of access and dissemination of information collected through data and telecommunications intercepts	12 hour maximum time from interception to translation of critical, time-sensitive intercepts	10% average improvement of time from intercept to translation	
2007	Protect the United States from terrorist attack	Incident response and investigative capability	100% response to requests for new quick reaction collection capability	Maintain 100% response to requests for new quick reaction collection capability	
2007	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	Title III system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2007	Establish an	Title 50 system	System certified	Maintain	

	enterprise-wide Security Program that protects our people, information, and *capabilities*	certification and accreditation	and accredited	certification and accreditation	
2007	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	DCS-3000 system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2008	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Automated voice to text tools available (language translation)	Initial automated voice to text tools available for Title 50 systems	10% improvement in voice to text tools capability	
2008	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Voice recognition tools available for Title 50 system	No voice recognition tools available for Title 50 systems	30% improvement in capability for voice recognition tools	
2008	Effectively utilize applied science and engineering resources to empower the FBI¿s *investigative and* intelligence operations and thwart the techniques of our adversaries	Improve speed of access and dissemination of information collected through *data and* telecommunications intercepts	10.8 hour maximum time from interception to translation of critical, time-*sensitive* intercepts	10% average improvement of time from intercept to translation	
2008	Protect the United States from terrorist attack	Incident response and investigative capability	100% response to requests for new quick reaction collection capability	Maintain 100% response to requests for new quick reaction collection capability	
2008	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	Title III system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2008	Establish an enterprise-wide Security Program that protects our people,	Title 50 system certification and accreditation	System certified and accredited	Maintain certification and accreditation	

	information, and capabilities				
2008	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	DCS-3000 system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2009	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Automated voice to text tools available (language translation)	Initial automated voice to text tools available for Title 50 systems	10% improvement in voice to text tools capability	
2009	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Voice recognition tools available for Title 50 system	No voice recognition tools available for Title 50 systems	30% improvement in capability for voice recognition tools	
2009	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Improve speed of access and dissemination of information collected through data and telecommunications intercepts	9.8 hour maximum time from interception to translation of critical, time-sensitive intercepts	10% average improvement of time from intercept to translation	
2009	Protect the United States from terrorist attack	Incident response and investigative capability	100% response to requests for new quick reaction collection capability	Maintain 100% response to requests for new quick reaction collection capability	
2009	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	Title III system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2009	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	Title 50 system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2009	Establish an	DCS-3000 system	System certified	Maintain	

	enterprise-wide Security Program that protects our people, information, and capabilities	certification and accreditation	and accredited	certification and accreditation	
2009	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Automated voice to text tools available (language translation)	Initial automated voice to text tools available for Title 50 systems	10% improvement in voice to text tools capability	
2010	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Automated voice to text tools available (language translation)	Initial automated voice to text tools available for Title 50 systems	10% improvement in voice to text tools capability	
2010	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Voice recognition tools available for Title 50 system	No voice recognition tools available for Title 50 systems	20% improvement in capability for voice recognition tools	
2010	Effectively utilize applied science and engineering resources to empower the FBI¿s investigative and intelligence operations and thwart the techniques of our adversaries	Improve speed of access and dissemination of information collected through data and telecommunications intercepts	9.8 hour maximum time from interception to translation of critical, time-sensitive intercepts	10% average improvement of time from intercept to translation	
2010	Protect the United States from terrorist attack	Incident response and investigative capability	100% response to requests for new quick reaction collection capability	Maintain 100% response to requests for new quick reaction collection capability	
2010	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	Title III system certification and accreditation	System certified and accredited	Maintain certification and accreditation	
2010	Establish an	Title 50 system	System certified	Maintain	

	enterprise-wide Security Program that protects our people, information, and capabilities	certification and accreditation	and accredited	certification and accreditation	
2010	Establish an enterprise-wide Security Program that protects our people, information, and capabilities	DCS-3000 system certification and accreditation	System certified and accredited	Maintain certification and accreditation	

All new IT investments initiated for FY 2005 and beyond must use Table 2 and are required to use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Please use Table 2 and the PRM to identify the performance information pertaining to this major IT investment. Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM. There should be at least one Measurement Indicator for at least four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov.

Performance Information Table 2:							
Fiscal Year	**Measurement Area**	**Measurement Category**	**Measurement Grouping**	**Measurement Indicator**	**Baseline**	**Planned Improvement to the Baseline**	**Actual Results**

I.E. Security and Privacy

In order to successfully address this area of the business case, each question below must be answered at the system/application level, not at a program or agency level. Systems supporting this investment on the planning and operational systems security tables should match the systems on the privacy table below. Systems on the Operational Security Table must be included on your agency FISMA system inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier).

All systems supporting and/or part of this investment should be included in the tables below, inclusive of both agency owned systems and contractor systems. For IT investments under development, security and privacy planning must proceed in parallel with the development of the system/s to ensure IT security and privacy requirements and costs are identified and incorporated into the overall lifecycle of the system/s.

Please respond to the questions below and verify the system owner took the following actions:

1. Have the IT security costs for the system(s) been identified and integrated into the overall costs of the investment:	Yes
a. If "yes," provide the "Percentage IT Security" for the budget year:	5
2. Is identifying and assessing security and privacy risks a part of the overall risk management effort for each system supporting or part of this investment.	Yes

3. Systems in Planning - Security Table:			
Name of System	**Agency/ or Contractor Operated System?**	**Planned Operational Date**	**Planned or Actual C&A Completion Date**
DCS-5000	Government Only	7/30/2008	1/30/2008

4. Operational Systems - Security Table:							
Name of System	**Agency/ or Contractor Operated System?**	**NIST FIPS 199 Risk Impact level**	**Has C&A been Completed, using NIST 800-377**	**Date C&A Complete**	**What standards were used for the Security Controls tests?**	**Date Complete(d): Security Control Testing**	**Date the contingency plan tested**
DCS-3000	Government Only	Low	Yes	6/1/2006	FIPS 200 / NIST 800-53	5/3/2006	6/27/2006
DCS-5000	Government Only	Moderate	Yes	2/3/2006	FIPS 200 / NIST 800-53	11/1/2005	6/27/2006
DCS-6000	Government Only	Low	Yes	6/2/2006	FIPS 200 / NIST 800-53	5/26/2006	6/27/2006

5. Have any weaknesses related to any of the systems part of or supporting this investment been identified by the agency or IG? Yes

a. If "yes," have those weaknesses been incorporated agency's plan of action and milestone process? Yes

6. Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses? No

a. If "yes," specify the amount, provide a general description of the weakness, and explain how the funding request will remediate the weakness.

7. How are contractor security procedures monitored, verified, validated by the agency for the contractor systems above?

Contractor security procedures are not required; systems that comprise the Digital Collection Project are agency owned and operated.

8. Planning & Operational Systems - Privacy Table:					
Name of System	**Is this a new system?**	**Is there a Privacy Impact Assessment (PIA) that covers this system?**	**Is the PIA available to the public?**	**Is a System of Records Notice (SORN) required for this system?**	**Was a new or amended SORN published in FY 06?**
DCS-3000	No	Yes.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
DCS-5000	No	Yes.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
DCS-6000	No	Yes.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.

I.F. Enterprise Architecture (EA)

In order to successfully address this area of the business case and capital asset plan you must ensure the investment is included in the agency's EA and Capital Planning and Investment Control (CPIC) process, and is mapped to and supports the FEA. You must also ensure the business case demonstrates the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

1. Is this investment included in your agency's target enterprise architecture?	Yes
a. If "no," please explain why?	
2. Is this investment included in the agency's EA Transition Strategy?	Yes
a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment.	Digital Collection Program
b. If "no," please explain why?	

3. Service Reference Model (SRM) Table:

Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.whitehouse.gov/omb/egov/.

Agency Component Name	Agency Component Description	Service Domain	FEA SRM Service Type	FEA SRM Component	FEA Service Component Reused Name	FEA Service Component Reused UPI	Internal or External Reuse?	BY Funding Percentage
		Back Office Services	Development and Integration	Legacy Integration			No Reuse	3
		Business Analytical Services	Reporting	Ad Hoc			No Reuse	5
		Digital Asset Services	Knowledge Management	Information Sharing			No Reuse	9
		Digital Asset Services	Knowledge Management	Knowledge Capture			No Reuse	52
		Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery			No Reuse	13
		Support Services	Search	Query			No Reuse	13

Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.

A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.

'Internal' reuse is within an agency. For example, one agency within a department is

reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.

Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the funding level transferred to another agency to pay for the service.

4. Technical Reference Model (TRM) Table:

To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.

FEA SRM Component	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (i.e. vendor or product name)
Knowledge Distribution and Delivery	Component Framework	Data Management	Database Connectivity	Microsoft
Knowledge Distribution and Delivery	Component Framework	Presentation / Interface	Content Rendering	Hyper Text Markup Language (HTML)
Knowledge Distribution and Delivery	Component Framework	Presentation / Interface	Dynamic Server-Side Display	Active Server Pages .Net
Knowledge Distribution and Delivery	Component Framework	Presentation / Interface	Dynamic Server-Side Display	Microsoft Sun Active Server Pages
Information Sharing	Service Access and Delivery	Access Channels	Other Electronic Channels	Uniform Resource Locator (URL)
Information Sharing	Service Access and Delivery	Access Channels	Other Electronic Channels	Web Service
Legacy Integration	Service Access and Delivery	Access Channels	Web Browser	Microsoft Internet Explorer
Legacy Integration	Service Access and Delivery	Access Channels	Web Browser	Netscape Navigator
Knowledge Distribution and Delivery	Service Access and Delivery	Service Requirements	Legislative / Compliance	Section 508
Knowledge Distribution and Delivery	Service Access and Delivery	Service Transport	Service Transport	Hyper Text Transfer Protocol (HTTP)
Knowledge Distribution and Delivery	Service Access and Delivery	Service Transport	Service Transport	Internet Protocol (IP)
Knowledge Distribution and Delivery	Service Access and Delivery	Service Transport	Service Transport	Transport Control Protocol
Knowledge Distribution and Delivery	Service Access and Delivery	Service Transport	Supporting Network Services	Simple Network Management Protocol (SNMP)
Query	Service Interface and Integration	Integration	Middleware	Database Access: ISQL/w
Query	Service Interface and Integration	Integration	Middleware	Database Access: PL/SQL
Knowledge	Service Interface	Integration	Middleware	Remote Procedure Call (RPC)

Distribution and Delivery	and Integration			
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Database / Storage	Database	Oracle
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Database / Storage	Database	Sybase
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Database / Storage	Storage	Compaq Enterprise Servers
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Delivery Servers	Application Servers	Compaq
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Delivery Servers	Web Servers	Apache
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Delivery Servers	Web Servers	Internet Information Server
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hewlett-Packard Hard Disk Drives
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hewlett-Packard Redundant Array of Independent Disks (RAID)
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Microprocessors
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Random Access Memory (RAM)
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Local Area Network (LAN)	Ethernet
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Local Area Network (LAN)	Virtual LAN (VLAN)
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Gateway
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Router
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Switch
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	ICTG T1 Card
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	ISDN
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Network Interface Card (NIC)
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Transceivers

Knowledge Distribution and Delivery	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Hewlett-Packard Printers

Service Components identified in the previous question should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications

In the Service Specification field, Agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.

5. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)?	No
a. If "yes," please describe.	
6. Does this investment provide the public with access to a government automated information system?	No
a. If "yes," does customer access require specific software (e.g., a specific web browser version)?	
1. If "yes," provide the specific product name(s) and version number(s) of the required software and the date when the public will be able to access this investment by any software (i.e. to ensure equitable and timely access of government information and services).	

Exhibit 300: Part II: Planning, Acquisition and Performance Information

II.A. Alternatives Analysis

Part II should be completed only for investments identified as "Planning" or "Full Acquisition," or "Mixed Life-Cycle" investments in response to Question 6 in Part I, Section A above.

In selecting the best capital asset, you should identify and consider at least three viable alternatives, in addition to the current baseline, i.e., the status quo. Use OMB Circular A- 94 for all investments, and the Clinger Cohen Act of 1996 for IT investments, to determine the criteria you should use in your Benefit/Cost Analysis.

1. Did you conduct an alternatives analysis for this project?	Yes
a. If "yes," provide the date the analysis was completed?	1/27/2006
b. If "no," what is the anticipated date this analysis will be completed?	
c. If no analysis is planned, please briefly explain why:	

2. Alternative Analysis Results: Use the results of your alternatives analysis to complete the following table:				
Send to OMB	**Alternative Analyzed**	**Description of Alternative**	**Risk Adjusted Lifecycle Costs estimate**	**Risk Adjusted Lifecycle Benefits estimate**
True	1- Volumetric Collection	Collection systems consolidated at locations requiring the largest number of collections and intercepts	167.653	0
True	2- End User Centric	Collection system deployment and support at locations containing the largest number of linguists (translators), case agents, and analysts.	152.202	0
True	3- High Input Capacity	Consolidated collections at locations with the largest capability for collections	167.933	0
True	Baseline	Digital collection support provided through distributed network of full scale, autonomous systems	72.5	0

3. Which alternative was selected by the Agency's Executive/Investment Committee and why was it chosen?

Alternative 1 - Volumetric Collection. An analysis found that a DCS-5000 regionalized architecture 1) reduces overhead costs, and 2) improves quality and performance by consolidating expertise and minimizing complexity. A cost-effectiveness analysis of 10 alternatives was performed using evaluation factors - user and system location(s), technology, and collection volume. Alt 1 was chosen. It addresses shortfalls including multiple independent systems, capacity underutilization, and costly support for each site. Top 3 are above.

4. What specific qualitative benefits will be realized?

The primary benefits of a regionalized architectural approach for the next generation of DCS-5000 would be to: 1) reduce overhead costs by utilizing "economies of scale" practices, and 2) improve quality and performance by consolidating expertise and minimizing complexity. Regionalization will improve the FBI's collection and processing capability through the deployment of digital collection systems that will provide continuous digital collection in the event of catastrophic failure of individual systems. A regionalized architecture would meet 17 of 17 strategies, business and technologies/vulnerabilities assessment criteria; the current distributed architecture met only 5 of 17 criteria. Qualitative benefits include: operations - 1) consolidation of locations permits majority of users to be collocated at few sites, 2) better utilization of system collection capacity, consolidated training; maintenance - 1) centralization of support resources, 2) fewer systems to maintain; accessibility - file transfers among sites more efficient, less resource intensive; 3) resiliency - decreased point of failure due from unplanned outages. Additionally, this regionalized infrastructure will be EDMS compatible and complementary. The long-term gains of a regionalized architecture would be to alleviate ongoing installation, upgrade, and maintenance costs associated with fielded systems. Staffing would also be reduced since Computer Specialists and Linguists would reside at the Regional Offices. Staffing would be minimal at the field office locations.

II.B. Risk Management

You should have performed a risk assessment during the early planning and initial concept phase of this investment's life-cycle, developed a risk-adjusted life-cycle cost estimate and a plan to eliminate, mitigate or manage risk, and be actively managing risk throughout the investment's life-cycle.

1. Does the investment have a Risk Management Plan? Yes

a. If "yes," what is the date of the plan? 5/12/2006

b. Has the Risk Management Plan been No

significantly changed since last year's submission to OMB?

c. If "yes," describe any significant changes:

Risks for the investment are identified within 3 categories: technical, acquisition, and financial. Each risk is evaluated as to its probability of occurrence and level of impact on schedule, cost, and technical performance to determine the overall risk rating. Given that, with very limited deviation, effort performed for digital collection implementation is completed by contracted support through firm fixed price contracts, there is limited risk associated with technical, cost and schedule performance. Baselines established are provided to contract vendors as contract requirements/deliverables; however, in order to mitigate the risk of unforeseen requirements and increased scope, a management reserve of 10% is maintained. Cost performance risk is mitigated through maximum usage of firm fixed price contracts and task orders. Budget projections are reviewed at least quarterly. Independent government cost estimates are developed, analyzed, and compared to contractor proposals for each major acquisition. Out-of-tolerance variances are brought to the contractors' attention and cost/price is negotiated.

2. If there currently is no plan, will a plan be developed?

a. If "yes," what is the planned completion date?

b. If "no," what is the strategy for managing the risks?

3. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule:

Risks for the investment are identified within 3 categories: technical, acquisition, and financial. Each risk is evaluated as to its probability of occurrence and level of impact on schedule, cost, and technical performance to determine the overall risk rating. Given that, with very limited deviation, effort performed for digital collection implementation is completed by contracted support through firm fixed price contracts, there is limited risk associated with technical, cost and schedule performance. Baselines established are provided to contract vendors as contract requirements/deliverables; however, in order to mitigate the risk of unforeseen requirements and increased scope, a management reserve of 10% is maintained. Cost performance risk is mitigated through maximum usage of firm fixed price contracts and task orders. Budget projections are reviewed at least quarterly. Independent government cost estimates are developed, analyzed, and compared to contractor proposals for each major acquisition. Out-of-tolerance variances are brought to the contractors' attention and cost/price is negotiated.

II.C. Cost and Schedule Performance

1. Does the earned value management system meet the criteria in ANSI/EIA Standard-748?	Yes

2. Answer the following questions about current cumulative cost and schedule performance. The numbers reported below should reflect current actual information. (Per OMB requirements Cost/Schedule Performance information should include both Government and Contractor Costs):

a. What is the Planned Value (PV)?	190314
b. What is the Earned Value (EV)?	186714
c. What is the actual cost of work performed (AC)?	188808
d. What costs are included in the reported Cost/Schedule Performance information (Government Only/Contractor Only/Both)?	Contractor Only
e. "As of" date:	3/2/2006
3. What is the calculated Schedule Performance Index (SPI= EV/PV)?	0.98

~~SECRET~~

4. What is the schedule variance (SV = EV-PV)?	-3600
5. What is the calculated Cost Performance Index (CPI = EV/AC)?	0.98
6. What is the cost variance (CV=EV-AC)?	-2094
7. Is the CV% or SV% greater than +/- 10%? (CV%= CV/EV x 100; SV%= SV/PV x 100)	No
a. If "yes," was it the?	
b. If "yes," explain the variance:	
c. If "yes," what corrective actions are being taken?	
d. What *is* most current "Estimate at Completion"?	472746
8. Have any significant changes been made to the baseline during the past fiscal year?	No
8. If "yes," when was it approved by OMB?	No

Comparison of Initial Baseline and Current Approved Baseline

25	DCS-6000 O&M	09/30/2011	$8.156	09/30/2011		$8.156				%
Project		**09/30/2011**	**$255.512**	**09/30/2011**	**09/30/2006**	**$255.512**	**$40.215**	**1826**	**$215.297**	**18.54**

~~SECRET~~

[redacted]OGC) (FBI)

From: [redacted](OGC) (FBI)
Sent: Friday, August 18, 2006 3:40 PM
To: CAPRONI, VALERIE E. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]
Cc: [redacted]OGC)(FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: FW: Post Cut Through Digits

b6
b7C

UNCLASSIFIED
NON-RECORD

FBI OGC ONLY.

See attached preliminary review of field offices. Keep in mind that this is a snapshot, looking from the network out, of what currently is being collected. A separate survey of the practices of TTAs in the field offices is also being amased.

None the less, it does seem to appear (at this point anyway with only 50% of the precints reporting) that, notwithstanding the DCS3000 default setting of not recording PCTDDs, a majority of offices are collecting PCTDDs, especially in classified investigations.

[redacted]

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 703 [redacted]

b6
b7C

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Friday, August 18, 2006 10:55 AM
To: [redacted]OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI); [redacted](OGC) (FBI); THOMAS, MARCUS C. (OTD) (FBI)
Subject: Post Cut Through Digits

UNCLASSIFIED
NON-RECORD

Gentlemen,

I checked all 56 field office's criminal pen-register DCS-3000 systems for post cut through dialed digit information. The attached spreadsheet list the field office and the observed data for the office. Rather than counting all targets with and without the dialed digit extraction option set I categorized the data as All, Most, Some, Few, and None. All means all targets in the system are currently set to collect post cut through digits. A ranking of Few means the majority of the targets are set with the option turned off. For example, WFO was ranked Few because only 6 out of 54 current targets were set to collect post cut through digits.

~~SECRET~~

A summary of the results:

Field offices with All targets set:
Field offices with Most targets set:
Field offices with Some targets set:
Field offices with Few targets set:
Field offices with No targets set:

b2
b7E

b6
b7C

Note the Cincinatti office currently does not have any targets.

Post Cut Thru.xls
(19 KB)

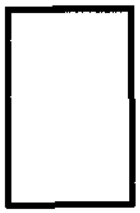
UNCLASSIFIED

UNCLASSIFIED

Office	Targets w/ Post-Cut Through Enabled
Albany	
Albuquerque	
Anchorage	
Atlanta	
Baltimore	
Birmingham	
Boston	
Buffalo	
Charlotte	
Chicago	
Cincinnati	
Cleveland	
Columbia	
Dallas	
Denver	
Detroit	
El Paso	
Honolulu	
Houston	
Indianapolis	
Jackson	
Jacksonville	
Kansas City	
Knoxville	
Las Vegas	
Little Rock	
Los Angeles	
Louisville	
Memphis	
Miami	
Milwaukee	
Minneapolis	
Mobile	
New Haven	
New Orleans	
New York	
Newark	
Norfolk	
Oklahoma Ci	
Omaha	
Philadelphia	
Phoenix	
Pittsburgh	
Portland	
Richmond	
Sacramento	
Salt Lake Cit	
San Antonio	
San Diego	
San Francisc	
San Juan	

b2
b7E

Seattle
Springfield
St. Louis
Tampa
WFO



b2
b7E

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, August 04, 2006 7:04 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] OGC) (FBI [redacted] OGC) (FBI)
Subject: PCTDD -- DCS 300

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

BTW [redacted]

b2
b7E
b5

UNCLASSIFIED

[redacted] (OGC) (FBI) ~~SECRET~~

From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 17, 2006 3:22 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Post-Cut-Through Digits Report---update

SECRET
RECORD 9999-7777

Thanks [redacted] all very good edits; how is this for fn 8?

[redacted]

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 17, 2006 2:31 PM
To: [redacted] OGC) (FBI)
Subject: RE: Post-Cut-Through Digits Report---update

SECRET
RECORD 9999-7777

I read through it twice and I think it is much improved from the first version in terms of explaining the process of collecting PCTDD. Unlike the first draft, I did not see any places where I thought the description sounded inconsistent with my understanding of how it all works.

I noticed a few places where I thought the drafting was a little unclear. I don't know how familiar the court is already with the concept of PCTDD, but I thought we could be clearer in few places, which I highlighted in this draft and provided some wording suggestions.

<< File: Post-Cut-Through Database Report-- v2 - lap 10172006 jdp.wpd >>

-----Original Message-----
From: [redacted] GC) (FBI)
Sent: Tuesday, October 17, 2006 10:19 AM
To: [redacted] GC) (FBI)
Subject: FW: Post-Cut-Through Digits Report---update
Importance: High

b6
b7C

SECRET
RECORD 9999-7777

[redacted]

I've redone the first 11 pages--and would appreciate your review as well. You can ignore the one I sent yesterday.

~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, August 18, 2006 3:40 PM
To: CAPRONI, VALERIE E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] OGC)(FBI); [redacted] OGC) (FBI); [redacted] OGC) (FBI); [redacted] OGC) (FBI); [redacted] OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: Post Cut Through Digits

b6
b7C

UNCLASSIFIED
NON-RECORD

FBI OGC ONLY.

[redacted]

b5

[redacted]

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703 [redacted]
Fax. 703

b6
b7C

-----Original Message-----
From: [redacted] (OTD) (FBI)
Sent: Friday, August 18, 2006 10:55 AM
To: [redacted] OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI); [redacted] OGC) (FBI); THOMAS, MARCUS C. (OTD) (FBI)
Subject: Post Cut Through Digits

UNCLASSIFIED
NON-RECORD

Gentlemen,

I checked all 56 field office's criminal pen-register DCS-3000 systems for post cut through dialed digit information. The attached spreadsheet list the field office and the observed data for the office. Rather than counting all targets with and without the dialed digit extraction option set I categorized the data as All, Most, Some, Few, and None. All means all targets in the system are currently set to collect post cut through digits. A ranking of Few means the majority of the targets are set with the option turned off. For example, WFO was ranked Few because only 6 out of 54 current targets were set to collect post cut through digits.

~~SECRET~~

A summary of the results:

Field offices with All targets set:
Field offices with Most targets set:
Field offices with Some targets set:
Field offices with Few targets set:
Field offices with No targets set:

b2
b6
b7C
b7E

Note the Cincinatti office currently does not have any targets.

Post Cut Thru.xls
(19 KB)

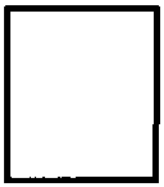
UNCLASSIFIED

UNCLASSIFIED

Office	Targets w/ Post-Cut Through Enabled
Albany	
Albuquerque	
Anchorage	
Atlanta	
Baltimore	
Birmingham	
Boston	
Buffalo	
Charlotte	
Chicago	
Cincinnati	
Cleveland	
Columbia	
Dallas	
Denver	
Detroit	
El Paso	
Honolulu	
Houston	
Indianapolis	
Jackson	
Jacksonville	
Kansas City	
Knoxville	
Las Vegas	
Little Rock	
Los Angeles	
Louisville	
Memphis	
Miami	
Milwaukee	
Minneapolis	
Mobile	
New Haven	
New Orleans	
New York	
Newark	
Norfolk	
Oklahoma City	
Omaha	
Philadelphia	
Phoenix	
Pittsburgh	
Portland	
Richmond	
Sacramento	
Salt Lake City	
San Antonio	
San Diego	
San Francisco	
San Juan	

b2
b7E

Seattle
Springfield
St. Louis
Tampa
WFO



b2
b7E

~~SECRET~~

From: [redacted]BA) (FBI)
Sent: Monday, August 21, 2006 5:30 PM
To: [redacted]BA) (FBI)
Subject: RE: phone

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Hello, I am the tech agent assigned to the case as depicted below.

[redacted]

In relation to the questions below, here is what I know:

1) SA [redacted] observations of his target who he knew to have several [redacted] cellular phones.

I have no idea where the information about "codes" came from.

SA [redacted] has provided me with this information after their most recent drug transaction with this subject.

2) Baltimore has tested a test phone with ERF where ERF has stripped off the full content.

There still is an issue with how the Telephone Application (TA) will differentiate between [redacted] and regular DNR type intercepts. Based upon the tests with ERF there is no way of letting TA know that this information came from a [redacted] service. [redacted] set up a separate client to allow us to be able to easily keep track of [redacted] DNR related information. However, TA cannot tell the difference between a [redacted] call" and a regular DNR.

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted](BA) (FBI)
Sent: Monday, August 21, 2006 12:29 PM
To: [redacted](BA) (FBI)
Subject: FW: phone

UNCLASSIFIED
NON-RECORD

FYI

SSA [redacted]
Squad 19
Baltimore Division
Office
Cell: [redacted]

~~SECRET~~

~~SECRET~~

[redacted](OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI); [redacted] (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); [redacted] (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] OGC) (FBI)
Cc: [redacted] CQ) (FBI); [redacted] (CQ) (FBI); [redacted] CO)(FBI); [redacted] (CQ) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI); [redacted] OCA) (FBI); [redacted] (ITD) (FBI)
Subject: [redacted] - No intercept requests since December Capability

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked [redacted] for releasing its [redacted] ervice without having first devised an intercept solution, and [redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request fo[redacted] since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

[redacted]

b5

From: [redacted]
T[redacted]
C[redacted]
Subject[redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] asked for update on [redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From[redacted] CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To[redacted] [CC]
> Subject: CALEA Update
> Importance: High
>
> [redacted]
>
> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 2004, [redacted] has not received any
> requests from law enforcement – federal or state – for the
> interception of [redacted] services o[redacted] data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted] working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. [redacted] does not know when FBI will be ready to begin

b2
b6
b7C
b7E

> routine (non-tes[redacted]nterceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703[redacted]
Fax. 703[redacted]

b2
b6
b7C
b7E

UNCLASSIFIED

> -----Original Message-----
> From: [redacted] [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [redacted] [CC]
> Subject: CALEA Update
> Importance: High
>
> [redacted]
>
> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 2004 [redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception of [redacted] data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted] is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. [redacted] does not know when FBI will be ready to begin
> routine (non-test) [redacted] interceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703 [redacted]
Fax. 70[redacted]

UNCLASSIFIED

UNCLASSIFIED

Having cajoled, warned and attacked [redacted] or releasing its [redacted] service without having first devised an intercept solution, an[redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request for [redacted] since the interim solution was enabled. b2 b7E

Rest assured that we will all hear this in testimony should legislation become and issue.

[redacted] b5

From [redacted]
To [redacted]
Cc [redacted]
Subject [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] asked for update on [redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From [redacted] [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To [redacted] [CC]
> Subject: CALEA Update
> Importance: High
>
> [redacted]
>
> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 2004 [redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception of [redacted] data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted] is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. [redacted] not know when FBI will be ready to begin
> routine (non-test) [redacted] interceptions.

b2 b5 b7C b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703 [redacted]
Fax. 70[redacted]

From:
To:
Cc:
Subject: CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

asked for update on eployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [CC]
> Subject: CALEA Update
> Importance: High
>
>
> Here is an update o Since deploying nationwide
> CALEA capabilities in December 2004 has not received any
> requests from law enforcement -- federal or state -- for the
> interception o ata services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. s working with FBI to coordinate "live" testing
> outside the Lab and is also working with the FBI to obtain handsets
> for the tests. does not know when FBI will be ready to begin
> routine (non-test interceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 70

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

out, I will, for my part, send it out via the GC to all CDCs and ask that the propagate it through the office and include it as an agenda item on their SACs Chiefs meetings.

From:
To
Cc
Subject: CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

b2
b6
b7C
b7E

I asked for update on deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [CC]
> Subject: CALEA Update
> Importance: High
>
>
>
> Here is an update on Since deploying nationwide
> CALEA capabilities in December 2004, has not received any
> requests from law enforcement -- federal or state -- for the
> interception of ata services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function; is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. does not know when FBI will be ready to begin
> routine (non-test nterceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 703

UNCLASSIFIED

UNCLASSIFIED

To: THOMAS, MARCUS C. (ITD) (FBI) (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI) ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI) ITD) (FBI) (OGC) (FBI)
Cc CQ) (FBI) (CQ) (FBI) CQ) (FBI) (CQ) (FBI); (ITD) (FBI); (ITD) (FBI); (OGC) (FBI) OCA) (FBI); ARRY (ITD) (FBI)
Subject: - No intercept requests since December Capability

b6
b5
b7C
b7E

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked for releasing its service without having first devised an intercept solution, and having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request for since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

b5

From:
To:
Cc:
Subject: CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

asked for update o deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: CC]
> Subject: CALEA Update
> Importance: High
>
>
>
> Here is an update on Since deploying nationwide
> CALEA capabilities in December 2004, has not received any
> requests from law enforcement -- federal or state -- for the
> interception o data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. does not know when FBI will be ready to begin
> routine (non-test) interceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 70[redacted]
Fax. 70[redacted]

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

From: [redacted] GC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI); [redacted] (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); [redacted] (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] CQ) (FBI); [redacted] CQ) (FBI); [redacted] CQ)(FBI); [redacted] (CQ) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI); [redacted] (OCA) (FBI); [redacted] (ITD) (FBI)
Subject: [redacted] No intercept requests since December Capability

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked [redacted] or releasing its [redacted] service without having first devised an intercept solution, and [redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request for [redacted] since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

[redacted]

b5

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

b2
b6
b7C
b7E

[redacted] I asked for update on [redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [redacted] C]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [redacted] CC]
> Subject: CALEA Update
> Importance: High
>
> [redacted]
>
> Here is an update on [redacted] Since deploying nationwide [redacted] CALEA capabilities in December 2004, [redacted] has not received any requests from law enforcement -- federal or state -- for the interception of [redacted] data services. I am told that FBI has been configuring its proprietary DS3000 collection function, [redacted] working with FBI to coordinate "live" testing outside the Lab, and is also working with the FBI to obtain handsets for the tests. [redacted] does not know when FBI will be ready to begin routine (non-test) [redacted] interceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 703

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

>
> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 200[redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception o[redacted]ata services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted]s working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests [redacted] does not know when FBI will be ready to begin
> routine (non-tes[redacted]nterceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

b2
b6
b7C
b7E

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703[redacted]
Fax. 70[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Monday, August 21, 2006 2:26 PM
To: [redacted]
Cc:
Subject: RE: [redacted] ssues List

b2
b6
b7C
b7E

[redacted]

"Appendix B" is a section of the TRAR (Testing Results Assessment Report). The TRAR was used in the early days of CALEA testing and includes a number of sections and Appendices that describe the Testing, Test Environment, Scheduling, Definitions, Results, etc. etc. The original documents ran hundreds of pages.

As we progressed, we have dispensed with all sections except "Appendix B". For consistency's sake, we have not changed the title. If we need to review former testing or results, we look in Appendix B. In the past several years, the testing results have been captured and placed in a stand-alone Appendix B, and that makes up the bulk of the information sent to the client. Specifically, Appendix B is the only information assembled by the test team for delivery to [redacted]

Nobody on the team corresponds in writing to the vendors. All correspondence relating to testing results is sent to the vendors and service providers by [redacted] an FBI employee, as opposed to any of us on the team, who are contractors.

I doubt that any mention of the DCS-3000 would have been made to [redacted] as that is an internal issue between the Test Team and TICTU. There is no good reason for [redacted] to have been informed about our internal dealings between groups. As far as written detail about comments regarding the Call Detail and Call Content separation, I am not aware of correspondence between [redacted] and [redacted] Appendix B is the information provided from the team. [redacted] will be a better source for an answer concerning the DCS-3000 and Call Detail / Call Content beyond Appendix B.

b2
b6
b7C
b7E

Your assumption regarding the CDC and CCC are correct. In the case of the [redacted] interim solution, everything came to us in a single data stream on one channel. The Data and Content were interspersed. In order to listen to the audio, we had to post-process, separate the Content, and run it through an audio decoder.

I believe your statement regarding CII is right on the money. All information is sent to the collection box [redacted] We undoubtedly referred to a CDC file and a CCC file in our analysis.

It is a correct statement to say that Law Enforcement must separate the Data from the Content. In order to get any kind of "Pen Register" data, the data stream would have to be post-processed by the collection system, and all non-Pen Register (Call Content related) information would have to be removed from the data received from [redacted]

I would encourage you to contac [redacted] directly for additional insight.

Regards,

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, August 21, 2006 1:15 PM

~~SECRET~~

~~SECRET~~

To: [redacted]
Cc: [redacted]
Subject: RE: [redacted] Issues List

Thanks [redacted] I see that this is "Appendix B" to something. I'm interested in everything that was communicated to [redacted] in this context. What was this document "Appendix B" to? Is it feasible to send me a copy?

I'm especially interested in anything that might've mentioned that DCS-3000 was being used in the testing, and anything that suggested that *another* deficiency was the inability to provide call detail isolated from call content. If there is anything in writing like that, I'd love to see it.

Separate question, just for the sake of my understanding: The document throughout refers to "CDC messages." [redacted]

b2
b6
b7C
b7E

-----Original Message-----
From [redacted]
Sent: Friday, August 18, 2006 2:23 PM
To [redacted]
Cc [redacted]
Subject: [redacted] Issues List

[redacted]

Attached is the Issues List for [redacted] testing performed in February, 2005.

Regards,

[redacted]

~~SECRET~~

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, August 04, 2006 7:04 PM
To: [redacted] OTD) (FBI)
Cc: [redacted] (OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] OGC) (FBI); [redacted] OGC) (FBI)
Subject: PCTDD -- DCS 300

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b5

BTW [redacted]

b2
b7E

UNCLASSIFIED

To: [redacted]
Cc: [redacted]
Subject: [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] I asked for update on [redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [redacted] CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [redacted] CC]
> Subject: CALEA Update
> Importance: High
>
[redacted]
>
> Here is an update on [redacted]. Since deploying nationwide [redacted]
> CALEA capabilities in December 2004 [redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception o[redacted]ata services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function[redacted] working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests [redacted] does not know when FBI will be ready to begin
> routine (non-te[redacted]nterceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703[redacted]
Fax. 703

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

****

This e-mail message and any attached files are confidential and are intended solely for the use of the addressee(s) named above. This communication may contain material protected by federal law and/or attorney-client, work product, or other privileges. If you are not the intended recipient or person responsible for delivering this confidential communication to the intended recipient, you have received this communication in error, and any review, use, dissemination, forwarding, printing, copying, or other distribution of this e-mail message and any attached files is strictly prohibited. If you have received this confidential communication in error, please notify the sender immediately by reply e-mail message and permanently delete the original message.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI); [redacted] (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); [redacted] (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] OGC) (FBI)
Cc: [redacted] CQ) (FBI); [redacted] (CQ) (FBI); [redacted] (CQ)(FBI); [redacted] CQ) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] OGC) (FBI); [redacted] (OCA) (FBI); [redacted] (ITD) (FBI)
Subject: [redacted] - No intercept requests since December Capability

b2 b6 b7C b7E

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked [redacted] or releasing it [redacted] service without having first devised an intercept solution, and [redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request fo[redacted] since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

b2 b6 b7C b7E b5

[redacted]

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] asked for update o[redacted] deployment and law enforcement use and learned the following.

~~SECRET~~

> -----Original Message-----
> From: [redacted] CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [redacted] CC]

> Subject: CALEA Update
> Importance: High
>
>
>
> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 2004 [redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception of [redacted] ata services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted] working with FBI to coordinate "live" testing
> outside the [redacted] nd is also working with the FBI to obtain handsets
> for the tests. [redacted] does not know when FBI will be ready to begin
> routine (non-test) [redacted] terceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703 [redacted]
Fax. 703 [redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

forwarding, printing, copying, or other distribution of this e-mail message and any attached files is strictly prohibited. If you have received this confidential communication in error, please notify the sender immediately by reply e-mail message and permanently delete the original message.

-----Original Message-----
From: (OGC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI); (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); (ITD) (FBI); (OGC) (FBI)
Cc: (CQ) (FBI); (CQ) (FBI); (CQ)(FBI); (CQ) (FBI); (ITD) (FBI); (ITD) (FBI); (OGC) (FBI); (OCA) (FBI); (ITD) (FBI)
Subject: No intercept requests since December Capability

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked or releasing its service without having first devised an intercept solution, and having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request fo since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

b1
b6
b7C
b7E
b5

From:
To:
Cc:
Subject: CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

asked for update on deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> T [CC]
> Subject: CALEA Update
> Importance: High
>

>
> Here is an update on Since deploying nationwide
> CALEA capabilities in December 2004, has not received any
> requests from law enforcement -- federal or state -- for the
> interception o data services. I am told
> that FBI has been configuring its proprietary DS3000 collection

> function. [redacted] working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. [redacted] does not know when FBI will be ready to begin
> routine (non-tes[redacted]terceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703[redacted]
Fax. 70[redacted]

b2
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

b2
b6
b7C
b7E

From: [redacted]CQ) (FBI)
Sent: Monday, March 14, 2005 2:33 PM
To: [redacted](OGC) (FBI); THOMAS, MARCUS C. (ITD) (FBI)[redacted] [redacted]ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI)[redacted](ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI)[redacted]TD) (FBI); [redacted](OGC) (FBI)
Cc: [redacted]GC) (FBI)[redacted](CQ) (FBI); [redacted]CQ) (FBI)[redacted](ITD) (FBI)[redacted] [redacted](OGC) (FBI)[redacted](OCA) (FBI)[redacted](ITD) (FBI)
Subject: RE:[redacted]- No intercept requests since December Capability

UNCLASSIFIED
NON-RECORD

[redacted]

I just forwarded you a copy (on your laptop computer) of the e-mail we sent to the Law Enforcement Technical Forum on

December 22 advising them that [redacted] Wireless and [redacted] now had a [redacted] solution and requesting that they include this feature on their court orders where required.

Thanks for volunteering to send it out to the FBI CDCs.

[redacted]
Unit Chief
CALEA Implementation Unit
(703) [redacted]

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI) [redacted] (ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI) [redacted] (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted] (ITD) (FBI) [redacted] (OGC) (FBI)
Cc: [redacted] (CO) (FBI); [redacted] (CO) (FBI); [redacted] (CO)(FBI); [redacted] (CQ) (FBI) [redacted] (ITD) (FBI); [redacted] (ITD) (FBI) [redacted] (OGC) (FBI); Jones, Darrin E (OCA) (FBI); [redacted] (ITD) (FBI)
Subject: [redacted] No intercept requests since December Capability

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked [redacted] or releasing its [redacted] ervice without having first devised an intercept solution, and [redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request for [redacted] since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

[redacted]

b2
b6
b7C
b7E
b5

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] asked for update o[redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [redacted] CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [redacted] [CC]
> Subject: CALEA Update
> Importance: High
>
> [redacted]

> Here is an update on [redacted] Since deploying nationwide [redacted]
> CALEA capabilities in December 2004 [redacted] has not received any
> requests from law enforcement -- federal or state -- for the
> interception of [redacted] data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. [redacted] is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests [redacted] does not know when FBI will be ready to begin
> routine (non-test) [redacted] interceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

b2
b6
b7C
b7E

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703.
Fax. 703 [redacted]

UNCLASSIFIED

UNCLASSIFIED

[redacted]GC) (FBI)

From: [redacted]GC) (FBI)
Sent: Monday, March 14, 2005 10:26 AM
To: [redacted](OGC) (FBI); THOMAS, MARCUS C. (ITD) (FBI) [redacted]ITD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); [redacted](ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted](ITD) (FBI [redacted] (OGC) (FBI)
Cc: [redacted](CQ) (FBI); [redacted](CO)VFBI); [redacted](CQ) [redacted]ITD) (FBI) [redacted]; [redacted](OGC) (FBI); [redacted](OCA) (FBI [redacted]TD) (FBI)
Subject: RE: [redacted] - No intercept requests since December Capability

b2
b6
b7C
b7E

[redacted]
[redacted]ITD) (FBI).v...

UNCLASSIFIED
NON-RECORD

[redacted]
Please calendar this item and get confirmation as soon as the order is issued.
Tell the CALEWG when that happens.

[redacted]OGC) (FBI)

From: [redacted]OGC) (FBI)
Sent: Thursday, March 10, 2005 9:55 AM
To: THOMAS, MARCUS C. (ITD) (FBI); [redacted]TD) (OGA); CLIFFORD, MICHAEL (ITD) (FBI); [redacted] (ITD) (FBI); DICLEMENTE, ANTHONY P. (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted]CQ) (FBI); [redacted] (CQ) (FBI); [redacted] (CQ) (FBI); [redacted] (CQ) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI); [redacted] OCA) (FBI); [redacted] (ITD) (FBI)
Subject: [redacted] - No intercept requests since December Capability

b2
b6
b7C
b7E

[redacted]
[redacted]TD) (FBI),v...

UNCLASSIFIED
NON-RECORD

Having cajoled, warned and attacked [redacted] for releasing its [redacted] service without having first devised an intercept solution, and [redacted] having rushed an interim solution into place this past December "at great expense", is now reporting that they have not received a single intercept request fo[redacted] since the interim solution was enabled.

Rest assured that we will all hear this in testimony should legislation become and issue.

[redacted]

b2
b6
b7C
b7E
b5

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: [redacted] CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

[redacted] I asked for update on [redacted] deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [redacted] [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> T[redacted] [CC]
> Subject: CALEA Update
> Importance: High
>
> Here is an update on [redacted] Since deploying nationwide [redacted] CALEA capabilities in December 2004 [redacted] has not received any requests from law enforcement -- federal or state -- for the interception o[redacted]ata services. I am told that FBI has been configuring its proprietary DS3000 collection function [redacted] working with FBI to coordinate "live" testing outside the Lab, and is also working with the FBI to obtain handsets for the tests. [redacted] does not know when FBI will be ready to begin

routine (non-test) [redacted] interceptions.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 70 [redacted]

b2
b6
b7C
b7E

UNCLASSIFIED

From: [redacted] (BA) (FBI)
Sent: Monday, August 21, 2006 5:30 PM
To: [redacted] (BA) (FBI)
Subject: RE: phone

UNCLASSIFIED
NON-RECORD

Hello, I am the tech agent assigned to the case as depicted below.

[redacted]

b2
b6
b7C
b7E

In relation to the questions below, here is what I know:

1) SA [redacted] observations of his target who he knew to have several [redacted] cellular phones.

I have no idea where the information about "codes" came from.

SA [redacted] has provided me with this information after their most recent drug transaction with this subject.

2) Baltimore has tested a test phone with ERF where ERF has stripped off the full content.

There still is an issue with how the Telephone Application (TA) will differentiate between [redacted] and regular DNR type intercepts. Based upon the tests with ERF there is no way of letting TA know that this information came from a [redacted] type service. [redacted] set up a separate client to allow us to be able to easily keep track of [redacted] DNR related information. However, TA cannot tell the difference between a [redacted] "call" and a regular DNR.

-----Original Message-----
From: [redacted] A) (FBI)
Sent: Monday, August 21, 2006 12:29 PM
To: [redacted] BA) (FBI)
Subject: FW: phone

UNCLASSIFIED
NON-RECORD

FYI

b6
b7C

SSA [redacted]
Squad 19
Baltimore Division
Offic
Cell: [redacted]

[redacted]GC) (FBI) SECRET

From: [redacted]OGC) (FBI)
Sent: Friday, August 18, 2006 3:55 PM
To: [redacted]OTD) (FBI); [redacted](OGC) (FBI)
Cc: [redacted](OTD) (FBI); [redacted](OTD) (FBI)
Subject: RE: Post-Cut-Though-Dialed Digits

SECRET
RECORD 66F-HQ-A1247863

Does the Field control the forwarding function from DCS3000 or can you over-ride that from ERF? b6 b7C

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 703

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Friday, August 18, 2006 3:44 PM
To: [redacted]GC) (FBI); [redacted]OGC) (FBI)
Cc: [redacted]OTD) (FBI); [redacted](OTD) (FBI)
Subject: RE: Post-Cut-Though-Dialed Digits

b6 b7C

SECRET
RECORD 66F-HQ-A1247863

The pen-register data forwarded from the DCS-3000 to the DCS-5000 and DCS-6000 systems is unfiltered, raw data. In most cases this information is associated with a full content intercept order. Occasionally, field offices elect to forward CALEA-based pen-register data obtained under FISA pen-register authority to the DCS-5000. In these cases, the PCTDD are delivered and collected by the DCS-5000 and eventually uploaded to TA.

[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, August 18, 2006 3:35 PM
To: [redacted]OGC) (FBI)
Cc: [redacted]OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI)
Subject: RE: Post-Cut-Though-Dialed Digits

SECRET
RECORD 66F-HQ-A1247863

I was under the impression from [redacted] that DCS3000 itself does keep all data in an administratively accessed file used for debugging, including PCTDD even when the default of do not record is selected. I thought I understoond [redacted] o say that that file is overwritten over time, but otherwise, if the do not record default remains unchanged, the

PCTDD does not go to TA or anywhere else.

[redacted]

Is this not correct?

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 70[redacted]
Fax. 70[redacted]

b6
b7C

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Friday, August 18, 2006 1:01 PM
To: [redacted]GC) (FBI)
Cc: [redacted]TD) (FBI)
Subject: RE: Post-Cut-Though-Dialed Digits

SECRET
RECORD 66F-HQ-A1247863

[redacted]

When DSC 3000 is used for a FISA collection, doesn't the DCS 3000 pass all to the [redacted]DSC 5000) including the PCTTD --in other words for FISAs the DCS3000 does NOT use the default of not recoding the PCTTD???? I might have this incorrect, but I thought there were some differences.

b6
b7C

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Thursday, August 17, 2006 10:05 PM
To: [redacted]OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC)(FBI); [redacted]OGC) (FBI); [redacted](OTD) (FBI); THOMAS, MARCUS C. (OTD) (FBI); [redacted](OGC) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]OGC) (FBI); CAPRONI, VALERIE E. (OGC) (FBI)
Subject: RE: Post-Cut-Though-Dialed Digits

~~SECRET~~
RECORD 66F-HQ-A1247863

FYI.

Since OTD only acquires the information and passes it along, and since the determination on whether one set of PCTDDs is content and not addressing, routing, dialing or signaling can only be made at the field office or analyst level, there really is nothing technologically speaking that can be done to ensure that content determined PCTDD is not used for investigative purposes.

However, OTD and STLU is proposing to amend the FD 871 which is required to be signed to authorize tech agents to implement a criminal or FISA PR to add a selection box requesting that PCTDD be recorded. That box will have an asterisk which near the signature line will alert approval signatories that "If Post Cut Through Dialed Digit (PCTDD) recording is required, approving authorities are certifying that they have read and will ensure compliance with the DOJ Deputy Attorney General's policy directive of May 24, 2004 prohibiting any investigative use of PCTDDs that are determined to qualify as content of

communications." In this way, there will at least be a record with a staff level supervisor, and ASAC acknowledging the DAG Directive each and every time they approve a pen register. In the absence of the box being checked, the DCS 3000 default of not recording PCTDDs will remain unchanged (although we still have the problem of non CALEA compliant provider networks were we cannot use the DCS 3000 and have to use older PR decoders that do not have the same ability to shut off recording of PCTDDs).

Please advise if you see any problems with this approach.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703[redacted]
Fax. 70[redacted]

b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, August 11, 2006 2:06 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OTD) (FBI); THOMAS, MARCUS C. (OTD) (FBI); [redacted](OGC) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); CAPRONI, VALERIE E. (OGC) (FBI)
Subject: Post-Cut-Though-Dialed Digits
Importance: High

OTHER outside the scope

SECRET
RECORD 66F-HQ-A1247863

[redacted]

~~SECRET~~

[redacted](OGC) (FBI)

From: [redacted]OGC) (FBI)
Sent: Wednesday, January 04, 2006 3:35 PM
To: [redacted](OGC) (FBI)
Subject: FW: State/Local Pen Orders

UNCLASSIFIED
NON-RECORD

[redacted] this is what I advised, is it correct?

b6
b7C

--It is STLU view that this encompasses surveillance assistance even when we retain custody and control of the equipment and just manage it for the benefit of the state/locals pursuant to a state/local order.

See below concern from the field--arguably if we retain custody and control of the equipment then we control its use, so most--if not all-- of the issues raised by the AG order (resource control, liability/legal authority to conduct surveillance, disclosure of technique, not use by others for other purposes, etc.) are not really issues when we decide if, when, whether, how the equipment will be used.

Your thoughts?

-----Original Message-----
From: [redacted](CE) (FBI)
Sent: Wednesday, January 04, 2006 1:55 PM
To: [redacted](OGC) (FBI)
Subject: RE: State/Local Pen Orders

UNCLASSIFIED
NON-RECORD

[redacted]

That's interesting. As you know, it is precisely FBI agents (TTAs) who are installing the equipment (DCS-3000) and participating in the surveillance (SAs reading off results of the pen to LEOs in the street and later processing the information for case purposes) without the three levels of approval noted in the policy. Will I now have to document each and every time we are instructed to ignore this policy? It is uncomfortable to be put in this position. I welcome your further comments.

[redacted]

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: [redacted]04, 2006 11:48 AM
To: [redacted](CE) (FBI)
Subject: RE: State/Local Pen Orders

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

Please note that the requirement to be named in the state court order is not a legal requirement but rather is an FBI policy requirement. In fact, the AG order No 1945-95 regarding the loan of ELSUR equipment in a state/local matter does NOT require that the state court order expressly authorize the FBI assistance. Instead, it provides only that (g) No Federal Bureau of Investigation personnel may be used to install the equipment or participate in the surveillance, unless deemed necessary and authorized by the Director or his designee. This restriction does not prohibit maintenance and repair of the equipment when not installed.

~~SECRET~~

~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 03, 2005 1:16 PM
To: [redacted] OGC) (FBI)
Subject: RE: AUSA Request for Expert Testimony

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] the AUSA, Peter Ko, called 3/4/05 to say that they have no intention of subpoenaing anyone, they believe they will get "enough of a stipulation" from the defense to introduce the T3 evidence and thinks they will have no problems getting the evidence in --that some how, this "got blown way out of proportion".....

-----Original Message-----
From: [redacted] (ITD) (FBI)
Sent: Monday, February 28, 2005 6:27 PM
To: [redacted] (ITD) (FBI); [redacted] (ITD) (FBI)
Cc: [redacted] (SD) (FBI [redacted] (ITD) (FBI) [redacted] (ITD) (FBI)
Subject: RE: AUSA Request for Expert Testimony

UNCLASSIFIED
NON-RECORD

[redacted]

Would you please screen this matter, make contact with the AUSA and let me know the gist of the AUSA's and TICTU's concern.

b6
b7C

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703 [redacted]
Fax. 703

-----Original Message-----
From: [redacted] (ITD) (FBI)
Sent: Monday, February 28, 2005 5:43 PM
To: [redacted] ITD) (FBI)
Cc: [redacted] (SD) (FBI); [redacted] (ITD) (FBI) [redacted] (ITD) (FBI)
Subject: AUSA Request for Expert Testimony
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted] TA [redacted] San Diego field office [redacted] has advised the following: AUSA Peter Ko, Southern District of California [redacted] is going to trial on bureau case 245D-SD-56228 [redacted]). This case was the subject of a T-III several years ago at which time data was obtained from [redacted] Wireless via the FBI's DCS-3000 network. This case goes to trial in about 2 weeks and the AUSA says the defense has not stipulated to the T-III. Therefore the AUSA has subpoenaed a witness from [redacted] Wireless and now wants to subpoena an expert witness from ITD-ERF to testify about the DCS-3000 network. This has been discussed with UC [redacted] and we believe that we probably do not testify about this type matter. The trial is set to begin 3/8/2005. We are seeking your advice or your direct contact with AUSA Ko. Tks.

b2
b6
b7C
b7E

[redacted]
Supervisory Special Agent
Telecommunications Intercept and Collection Technology Unit (TICTU)
Electronic Surveillance Technology Section
Investigative Technology Division
Quantico, Virginia
703 [redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Thursday, August 05, 2004 10:16 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (SecD) (CON); [redacted] (OGC) (FBI); [redacted] (ITD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] A. (OTD) (FBI)
Subject: Pen Register, [redacted] Telephone Applications

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

[redacted]

I am [redacted] newly assigned Unit Chief for the Telecommunications Intercept and Collection Technology Unit (TICTU) at ERF. This unit is responsible for providing electronic surveillance equipment to all FBI field offices. This equipment ranges from the 1033 unit, the [redacted] DCS-3000 (switched based equipment), the DCS-5000 (FISA platform), and the DCS-6000 (criminal platform). I am contacting you to schedule a meeting of all parties listed in the cc: (and any you deem necessary) to meet here at ERF and work towards written guidance with the [redacted] FISA incoming data and what classification before telephone applications.

TICTU is currently receiving increased communications from the field offices as to the direction to follow. I am providing two possible dates to meet: Thursday, August 26, at 10:00 a.m. or Friday, September 3rd at 10:00 a.m. Please advise of the date you prefer, and if additional information is needed before we meet. I can be contacted via e-mail or by telephone 703 [redacted] I await your response.

[redacted]

SENSITIVE BUT UNCLASSIFIED

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, February 17, 2006 3:28 PM
To: [redacted] (OGC) (FBI)
Subject: RE: More databases

UNCLASSIFIED
NON-RECORD

b6
b7C

Thanks. From my point of view, it means NO MORE DESCRIPTIONS NEED TO BE ADDED from that list, at least.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, February 17, 2006 3:17 PM
To: [redacted] (OGC) (FBI)
Subject: RE: More databases

UNCLASSIFIED
NON-RECORD

[redacted]

This is what I've learned from OTD:

Most wireless carriers have centralized their CALEA delivery points. In most cases, CDC information **(pen-register/trap-trace data) for all FBI intercepts per carrier are delivered to one FBI gateway per carrier**. The locations of the gateways vary and depend on the location and connection restrictions imposed by the carriers. **DCSnet** is a peerless and private IP network that **supports the delivery and transport of CALEA-enabled intercept product from the FBI gateways to all 56 FBI field offices**. It is an unclassified network, and is not used to transfer processed/collected ELSUR information--Nor is it in itself a collection system--the collection system is the DCS-3000.

The DCS-3000 is a suite of software applications that support the FBI's CALEA-based intercepts. This suite of applications has two primary functions: 1) a gateway between all carriers' delivery systems and the FBI's collection systems and centers (e.g., DCS-5000 in Atlanta Division), and 2) the primary collection system for all CALEA-enabled criminal pen-register and trap/trace intercepts.

As I understand, the DCS-3000 serves as a gateway between carriers and the DCS-5000 system for security reasons. In essence, Security division will not allow a classified collection system to have connection to the outside--hence the DCS-3000 serves as the link and is for that purpose just a transport of the FISA material from the carrier to the DCS-5000 system.

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Wednesday, February 15, 2006 11:04 AM
To: [redacted] OGC) (FBI)
Subject: More databases

UNCLASSIFIED
NON-RECORD

Have your heard of the Data Collection System Network (DCSNET) or the Rapid Prototyping Facility Network (RPFNET). Also , are DCS 3000 and DCS 5000 variations of each other, as far as pen register collection.

I have reading a list of databases that the Security Division sent so that's where these issues are coming from. Thanks. pik

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted](OGC) (FBI)

From: [redacted](OTD) (FBI)
Sent: Friday, February 10, 2006 8:27 AM
To: [redacted](OGC) (FBI)
Cc: [redacted](OTD) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

[redacted]ou are correct in your definition of the [redacted]It receives pen register data from sources such as the Remote DNR and the DCS 3000 and enables the Elsur Tech to upload the data to Telephone Applications from one location. The system also allows the operator to program the Remote DNR's as well. [redacted]

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Thursday, February 09, 2006 5:37 PM
To: [redacted]OTD) (FBI)
Subject: FW:

UNCLASSIFIED
NON-RECORD

[redacted]

Please review and advise [redacted]

Thanks,

[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, February 09, 2006 1:40 PM
To: [redacted](OTD) (FBI)
Subject: FW:

UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

Please advise if correct- what does the [redacted]do? -thanks [redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, February 09, 2006 10:03 AM
To: [redacted](OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

The [redacted]nd DCS 3000 are PEN REGISTER collections---not content!!!! Yes the field elsur tech downloads the pen data and then uploads it into TA for analysis but the SMP does NOT apply to Pen Register data correct?

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, February 09, 2006 9:14 AM

~~SECRET~~

To: [redacted]GC) (FBI)
Subject: RE:

~~SECRET~~

UNCLASSIFIED
NON-RECORD

Let me clarify something, however. The field offices are telling me with respect to these databases that a certain number of people have access to these databases, so they are not simply collection devices, if people can access them and view data. People are having access to raw FISA data, correct?

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Thursday, February 09, 2006 9:05 AM
To: [redacted](OGC) (FBI)
Subject: RE:

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

The [redacted]s a pen register collection system--similar to DSC-3000--but its older and doesn't do everything that DSC-3000 does (e.g., can't understand [redacted]codes and some of the other CALEA provided data), so I believe that it is being phased out

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Thursday, February 09, 2006 8:51 AM
To: [redacted](OGC) (FBI)
Cc: [redacted]OGC)(FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

Thanks. How about [redacted] or a system labeled simply as [redacted]by Baltimore)_

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, February 09, 2006 8:48 AM
To: [redacted]OGC) (FBI)
Cc: [redacted](OGC)(FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

[redacted]

b2
b6
b7C
b7E
b5

DCS-3000 is the Collection system for pen data--to the extent it collects content it's limited to SMS (text messages)--but it serves only as the collection point--the data is passed to another system (TA etc for analysis).
PenLink is a software application that can be used to help analyze pen data.
[redacted]
Analyst Notebook (I-1) appears to be a software application that can be used with Choicepoint According to the following link (This is software that can be installed on FBINET. It allows for the input of data for graphical display and analysis. Pen-link data can be imported into i2 Notebook.) [redacted]

~~SECRET~~

[redacted]

-----Original Message-----
From: [redacted] GC) (FBI)
Sent: Thursday, February 09, 2006 8:33 AM
To: [redacted] OGC) (FBI); [redacted] OGC)(FBI)
Subject:

b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Anyone know what DCS-3000, Penlink, [redacted] Analyst Notewoork (I-1) are. These are all new ones that are coming up in the course of reading field office responses.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, February 09, 2006 10:52 AM
To: [redacted] OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

You're right. I missed that. SMP does not apply to pen registers.

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, February 09, 2006 10:03 AM
To: [redacted] (OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

The [redacted] and DCS 3000 are PEN REGISTER collections---not content!!!! Yes the field elsur tech downloads the pen data and then uploads it into TA for analysis but the SMP does NOT apply to Pen Register data correct?

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, February 09, 2006 9:14 AM
To: [redacted] (OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Thursday, February 09, 2006 9:05 AM
To: [redacted] OGC) (FBI)
Subject: RE:

b2
b6
b7C
b7E
b5

UNCLASSIFIED
NON-RECORD

The [redacted] is a pen register collection system--similar to DSC-3000--but its older and doesn't do everything that DSC 3000 does (e.g., can't understand [redacted] codes and some of the other CALEA provided data), so I believe that it is being phased out

-----Original Message-----
From: [redacted] GC) (FBI)
Sent: Thursday, February 09, 2006 8:51 AM
To: [redacted] OGC) (FBI)
Cc: [redacted] OGC)(FBI)
Subject: RE:

UNCLASSIFIED

NON-RECORD

Thanks. How about [redacted] or a system labeled simply as "3094" (by Baltimore)_

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, February 09, 2006 8:48 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC)(FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

This is the risk with getting input from the field--it appears they didn't understand the question. The items below are not database systems that contain raw FISA material (i.e. content) that must be minimized under the SMP (unless minimization applies to pen data and to [redacted]

b2
b6
b7C
b7E

[redacted]

DCS-3000 is the Collection system for pen data--to the extent it collects content it's limited to SMS (text messages)--but it serves only as the collection point--the data is passed to another system (TA etc for analysis).
PenLink is a software application that can be used to help analyze pen data.
[redacted]
Analyst Notebook (I-1) appears to be a software application that can be used with Choicepoint According to the following link (This is software that can be installed on FBINET. It allows for the input of data for graphical display and analysis. Pen-link data can be imported into i2 Notebook [redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, February 09, 2006 8:33 AM
To: [redacted] (OGC) (FBI) [redacted] GC)(FBI)
Subject:

UNCLASSIFIED
NON-RECORD

Anyone know what DCS-3000, Penlink, [redacted] Analyst Notewoork (I-1) are. These are all new ones that are coming up in the course of reading field office responses.

b2
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] OGC) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Wednesday, November 02, 2005 5:12 PM
To: [redacted] (OGC) (FBI)
Subject: RE: FISC database response

SECRET
RECORD 319 xx

b2
b6
b7C
b7E

[redacted]

The document is correct in my view. I am not sure what you mean by "original". The intercept data are delivered from the carriers' intercept access points to us in "raw" formats. The DCS-3000 decodes these formats and presents the information in "human readable" format. The "human readable" formatted information is typical uploaded to TA by either saving the data to a removeable disk (we've always considered this to be the "original") or through an automatic connection to th[redacted] most field offices prefer the [redacted] ethod). If the [redacted] is used and the data is not saved to a removeable disk, the data remains on the DCS-3000 indefinitely.

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, November 01, 2005 4:33 PM
To [redacted] (OTD) (FBI)
Subject: FW: FISC database response

SECRET
RECORD 319 xx

[redacted]

would you review the discussion of DCS-3000. make sure it explains how FISA information in DCS-3000 is handled, including the manner in which it can be searched and retrieved. Also Is the raw pen register data stored in the DCS-3000 system or just collected there and then the original sent some place else for storage. If stored there, for how long is the original maintained?

b6
b7C

thanks,

[redacted]

-----Original Message-----
From [redacted] OGC) (FBI)
Sent: Tuesday, November 01, 2005 4:09 PM
To: [redacted] (OGC) (FBI) [redacted] OGC)(FBI)
Subject: RE: FISC database response

SECRET
RECORD 319 xx

Here's a few more edits. It doesn't include the portion markings and it's still not clear to me what the interplay is between EDMS and DWS with respect to email and chat collections. As it reads now, it appears that some (CT collections go into DWS and others into EDMS?) perhaps STAS can clarify.

~~SECRET~~

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, November 01, 2005 11:43 AM
To: [redacted] (OGC) (FBI)
Subject: FW: FISC database response

SECRET
RECORD 319 xx

[redacted] apologize, I inadvertently left you off of this email.
Please let me know whether you can look at this. Also, please refer to the 1101 version that I have attached rather than the 1031 one.
thanks
vpc

b6
b7C

[redacted]
Assistant General Counsel
Policy & Training Unit
National Security Law Branch
(202) 32[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, October 31, 2005 2:16 PM
To: [redacted] (CyD) (FBI); [redacted] DI) (FBI); [redacted] OTD) (FBI); [redacted] (CyD) (FBI); THOMAS, MARCUS C. (OTD) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] OGC) (FBI); [redacted] (CD) (FBI); [redacted] (OGC)(FBI); [redacted] (CD) (FBI); [redacted] (OGC) (FBI)
Subject: FISC database response

SECRET
RECORD 319 xx

[redacted]

b2
b6
b7C
b7E
b5

[redacted]

b2
b6
b7C
b7E
b5

[redacted]
Assistant General Counsel
Policy & Training Unit
National Security Law Branch
(202) 324-[redacted]

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~SECRET~~

[redacted]OGC) (FBI)

From: [redacted]CQ) (CON)
Sent: Wednesday, September 28, 2005 1:37 PM
To: [redacted](OGC) (FBI)
Subject: FW[redacted] and Location

b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

See [redacted] remark below. There is no reference I can provide regarding this non-standard feature. The ServingSystem Message identifies a carrier's network. It is used to identify the network of a carrier to which a subject has roamed.

[redacted]

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Wednesday, September 28, 2005 1:33 PM
To: [redacted](CQ) (CON)
Subject: RE: [redacted]nd Location

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]switches also provide th[redacted]nformation in the Serving System message. We have modified our DCS-3000 system to exploit this "non-standard" feature.

[redacted]

b6
b7C
b7E

-----Original Message-----
From: [redacted](CQ) (CON)
Sent: Wednesday, September 28, 2005 12:38 PM
To: [redacted](OGC) (FBI); [redacted](OTD) (FBI)
Cc: [redacted]CQ) (FBI); CLIFFORD, MICHAEL (OTD) (FBI); [redacted](OTD) (FBI); [redacted]L. (OTD) (FBI)
Subject: FW: [redacted] and Location

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]h,

I forgot to provide the reference for J-Standard:

[redacted]

If you go the the TIA website and search [redacted]ou'll be rewarded with

it through the office and include it as an agenda item on their SACs Chiefs meetings.

From:
To:
Cc:
Subject: CALEA Update
Date: Tuesday, March 08, 2005 11:11 AM

I asked for update on deployment and law enforcement use and learned the following.

> -----Original Message-----
> From: [CC]
> Sent: Tuesday, March 08, 2005 10:53 AM
> To: [CC]
> Subject: CALEA Update
> Importance: High
>
>
>
> Here is an update on . Since deploying nationwide
> CALEA capabilities in December 2004 has not received any
> requests from law enforcement -- federal or state -- for the
> interception of data services. I am told
> that FBI has been configuring its proprietary DS3000 collection
> function. is working with FBI to coordinate "live" testing
> outside the Lab, and is also working with the FBI to obtain handsets
> for the tests. does not know when FBI will be ready to begin
> routine (non-test) interceptions.

b2
b6
b7C
b7E

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. 703
Fax. 703

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

From: [redacted] (BA) (FBI)
Sent: Monday, August 21, 2006 5:30 PM
To: [redacted] BA) (FBI)
Subject: RE: phone

UNCLASSIFIED
NON-RECORD

Hello, I am the tech agent assigned to the case as depicted below.

[redacted]

b2
b6
b7C
b7E

In relation to the questions below, here is what I know:

1) SA [redacted] observations of his target who he knew to have several [redacted] ellular phones.

I have no idea where the information about "codes" came from.

SA [redacted] has provided me with this information after their most recent drug transaction with this subject.

2) Baltimore has tested a test phone with ERF where ERF has stripped off the full content.

There still is an issue with how the Telephone Application (TA) will differentiate betwee [redacted] and regular DNR type intercepts. Based upon the tests with ERF there is no way of letting TA know that this information came from a [redacted] type service [redacted] set up a separate client to allow us to be able to easily keep track of [redacted] DNR related information. However, TA cannot tell the difference between a [redacted] "call" and a regular DNR.

-----Original Message-----
From: [redacted] (BA) (FBI)
Sent: Monday, August 21, 2006 12:29 PM
To: [redacted] BA) (FBI)
Subject: FW: phone

b6
b7C

UNCLASSIFIED
NON-RECORD

FYI

SSA [redacted]
Squad 19
Baltimore Division
Office: [redacted]
Cell:

~~SECRET~~

Step 8. Case Squad designates individual(s) to operate the Pen Register (DCS 3000 system) located on the third floor (T-3 space).

Step 9. Case squad provides signed Pen Register/2703(d) Order to IS-2.

Step 10. Both the case squad and IS-1 shall evaluate the active and historical pen register information to determine the logical location to begin searching, i.e. latest specific cell cite and sector, on/off, times, etc.

Step 10. Case Agent assigned to Pen Register maintains contact with IS-1 tracking team and provides update as to target's cell phone use.

IS-1 conducts live tracking operation.

Recommendations: Any case squad that foresees the use of Pen Registers and Provider information for cell tracking purposes should:

a. Maintain a file of pony Pen Register/2703(d) Orders for the major cellular providers. Ponies can be obtained from IS-2.
b. Pro-actively meet with their perspective AUSA's and discuss specifics of Order.
c. Ensure squad members are familiar with the use of the DCS-3000/Pen Registers.

I. **(U) DEFINITIONS** (As defined by the Federal Bureau of Investigation's Office of the Chief Information Officer/Office of IT Policy & Planning/ Enterprise Architecture Unit):

A. SYSTEM: An integrated aggregation of electronic devices, interfaces, software, and support functions designed to fulfill a specific mission requirement. A system may include equipment, trained personnel, facilities, data and procedures, and software. For project purposes, a system is typically defined as the highest level of hardware organization composed of multiple subsystems. Boundaries must be defined in defining a system for certification and accreditation.

B. APPLICATION: IT (Informational Technology) assets that are included in a system to perform a specific function(s). For example, application software includes database programs, word processors, and spreadsheet programs.

C. DATABASE: A collection of data stored electronically that is accessed by a processor to perform a function.

D. NETWORK: A group of computers linked together to exchange and share information. Networks can consist of a number of linked computers in a specific physical location, a Local Area Network (LAN), or they may consist of computers located at different physical sites linked together by means of phone lines and modems or other forms of long distance communications.

II. SYSTEMS DESCRIPTION REQUEST FROM OIPR: EDMS & DWS

A. Electronic Surveillance (ELSUR) Data Management System (EDMS)

1. Description of the types of Foreign Intelligence Surveillance Act (FISA) information contained in EDMS.

(U) EDMS contains ELSUR products from counterterrorism (CT) and counterintelligence (CI) field collection systems involving:

- Audio – copies of microphone surveillance and telephony audio, for a limited number of cases.
- Email and chat – EDMS is an original collector of raw email and chat communications
- Raw pen register data —for a limited number of cases originating from Red Wolf (See Section III.A.1)
- Test pen register data —for limited testing from DCS-3000 (See Section III.A.3)
- Raw seized media—for a limited number of CT cases.
- Minimized translation summaries (tech cuts)

a. Description of the types of FISA information contained in [redacted]

[redacted]

b2
b7E

b. Explanation of how access to FISA information is controlled, that is, restrictions on search and retrieval of information.

(U) (S) Access to FISA facsimiles is generally restricted to predetermined authorized users generally linguists assigned to the case, the linguist's supervisor, the Case Agent, and the system administrator in the office where the data is collected. [redacted]

c. Implementation of standard minimization procedures.

b2
b7E

[redacted]

3. DCS-3000 (system)

a. Description of the types of FISA information contained in DCS-3000.

(U) DCS-3000 is the primary collection platform for pen-register/trap-trace data pursuant to the Communications Assistance for Law Enforcement Act of 1994 (CALEA), and this is the only information collected by the DCS-3000. Per the CALEA, this information is intercepted by the targets' service providers based on target telephone number and delivered to the DCS-3000 in standard formats. The

information is stored in text-formatted files for each target telephone number.

b. Explanation of how FISA information is controlled, that is, restrictions on search and retrieval of information.

(U) Most FBI field offices use the DCS-3000 as a "front-end" collector. The pen-register/trap-trace data collected by the DCS-3000 is typically manually uploaded to the Telephone Application (TA) database at FBI Headquarters, through which it can then be searched. The DCS-3000 team is working in conjuncture with EDMS (See Section II.A) to provide for an automatically pen-register upload to TA. The DCS-3000 also has a rudimentary report generation feature and simple text-based search tools for use by Technically Trained Agents and system administrators.

c. Implementation Of Standard Minimization Procedures.

(S) (U) The DCS-3000 collects only pen-register/trap-trace information.

(S)

OTHER outside the scope

INVESTIGATIVE TECHNOLOGY DIVISION'S

TECHNICALLY TRAINED AGENT MANUAL

➢ **MANUALS:** For traditional DNR equipment Manuals see:

[redacted]

- For details regarding the DCS-6000, go to the TICTU Website at

[redacted]

➢ **MANUALS:** For major Pen Register/Trap-Trace collection platform Manuals see:

[redacted]

· ***Switch-based:*** In implementing switch-based Pen Registers and/or Traps and Traces, TTAs frequently utilize the Data Collection System (DCS)-3000 application suite and/or the criminal law-based (JSI) DCS-6000 ("Voice Box") platform. In other conventional (non-CALEA) switch-based Pen Register/Trap and Trace cases, the interface for collecting such information may be one of the Pen Register DNR platforms produced by JSI.

- For details regarding the DCS-3000 system, go to the TICTU Website and consult the Switch-Based Intercept Team at [redacted]

- For details regarding the DCS-6000 system, go to the TICTU Website and consult the [redacted]

b2
b7E

➢ **MANUALS:** For major Pen Register/Trap-Trace collection platform Manuals see:

[redacted]

- For details regarding more conventional (non-CALEA) DNR equipment and DNR platforms, etc., go to the TICTU Website and consult the Traditional Technologies Intercept Team at [redacted]

➢ **MANUALS:** For traditional DNR equipment Manuals see:

[redacted]

· ***Network/Wireline Data-based:*** In implementing Network or Wireline Data-related Pen Registers and/or Traps and Traces, such Pen Registers and/or Traps and Traces are frequently implemented by service providers using their own proprietary or commercially-available equipment. In some cases, the FBI (DITU), or specially-trained TTAs, can also effect such Pen Registers and/or Traps and Traces utilizing tools commercially-available to law enforcement, such as "[redacted]" Processing and viewing systems/tools such as [redacted] and "[redacted]" are also used.

- For details regarding the use of "products" such as [redacted] go to the DITU Website at [redacted]

➢ **MANUALS:** For Manuals regarding products such as [redacted] go to the DITU Website at [redacted]

· ***High-Capacity -based:*** In implementing High-capacity-based Pen Registers and/or Traps and Traces, such Pen Registers and/or Traps and Traces are frequently implemented by TTAs in concert

Such nondisclosure pertains to details (including display) of this material. General descriptions or disclosures as to the overall technical functionality/operation of technical equipment or techniques are not prohibited. Any potential departure from this policy must be specifically approved by ITD at a unit chief or higher level before disclosure is made. See MIOG, Part 2, 10-10.13(4).

· ***FBI Testimony***: As set forth in MIOG, Part 2, 16-4.16, expert testimony, regarding Pen Registers and/or Traps and Traces or otherwise, is available from the Investigative Technology Division (ITD). Such requests may emanate from Federal or State prosecutors or defense counsel. In a number of cases, such ITD personnel may be qualified to testify as subject matter experts in a given area within the Technical Investigative Program (TIP). In other cases, it would be more appropriate for non-FBI personnel, such as personnel from communications service providers, equipment manufacturers, software vendors, etc., to testify as experts in a given area of expertise.

The procedures for FBI technical personnel who testify as subject matter experts within the FBI's TIP are the same as those that apply to other FBI witnesses, including adherence to the dictates of 28 C.F.R.§ 16.21 et seq. Any legal or procedural questions should be promptly brought to the attention of the appropriate Assistant United States Attorney (AUSA) and the appropriate field office CDC or to an attorney in the Technology Law Unit, Office of the General Counsel, FBIHQ.

m) Evidence Acquisition/Recordation/Handling:

Pen Registers and Traps and Traces acquire dialed number as well as other call-control signaling information. Pen Register equipment used in local loop interceptions typically captures audio tones/signaling that is then portrayed as dialed numbers and/or other call-control indicators. Under CALEA, which is carrier (and principally switch)-based, the Pen Register and/or Trap and Trace information acquired is referred to as "call-identifying information (CII)." Under CALEA, delivery of CII to law enforcement is made over a "call data channel (CDC)." Details as to the elements/ format/messages for CALEA-compliant Pen Register and/or Trap and Trace uses in wireline and wireless networks are set forth in the J-STD-025.

The interface for collecting such Pen Register and/or Trap and Trace information may be DNR platforms such as those produced by JSI or the CALEA-related DCS-3000 platform, which may connected to the DCS-6000 (Voice Box).

Once Pen Register and/or Trap and Trace information is acquired, the signaling information should be recorded electronically as the "original evidence." Electronic recordation can be accomplished through recorders attached to Pen Register/Trap and Trace DNR platforms such as those produced by JSI or the CALEA-related DCS-3000 platform or the DCS-6000 (Voice Box).

Hardcopy printouts from the original electronic signaling may also constitute "original evidence." However, *post-processed* (manipulated) Pen/Trap printout information, such as that produced through the "Telephone Application (TA)," while user-friendly for investigators and prosecutors, is technically not original evidence because it has been processed/manipulated by the TA program. If TTAs handle Pen Register/Trap evidence, they run the risk of becoming part of the "chain of custody" for the Pen/Trap evidence, thus exposing themselves to the possibility of having to testify (contrary to FBI policy). Hence, TTA involvement in evidence handling must be avoided.

i) Equipment/Software/Tools (E/S/T); Technical Manuals:

For FISA law-based Pen Registers and/or Traps and Traces, various equipment, software, and tools (E/S/T) are used in the technical implementation. The E/S/T and its specifications and the technical manuals regarding the E/S/T, including maintenance, are addressed below.

· ***Local Loop-based:*** In implementing local loop Pen Registers, the interface for collecting such information may be one of the traditional Pen Register/DNR systems produced by JSI or the FISA law-based (Raytheon) DCS-5000 ([redacted] platform.

- For details regarding traditional DNR equipment and DNR systems, etc., go to the TICTU Website and consult the Traditional Technologies Intercept Team at [redacted]

  - **MANUALS:** For traditional DNR equipment Manuals see: [redacted]

- For details regarding the DCS-5000, go to the TICTU Website and consult the [redacted]

  - **MANUALS:** For major Pen Register/Trap-Trace collection platform Manuals see: [redacted]

· ***Switch-based:*** In implementing switch-based Pen Registers and/or Traps and Traces, TTAs frequently utilize the Data Collection System (DCS)-3000 application suite and/or the FISA law-based (Raytheon) DCS-5000 ("Red Wolf") platform. In other conventional (non-CALEA) switch-based Pen Register/Trap and Trace cases, the interface for collecting such information may be one of the Pen Register DNR platforms produced by JSI.

b2
b7E

- For details regarding the DCS-3000 system, go to the TICTU Website and consult the Switch-Based Intercept Team at [redacted]

- For details regarding the DCS-5000 system, go to the TICTU Website and consult the [redacted]

  - **MANUALS:** For major Pen Register/Trap-Trace collection platform Manuals see: [redacted]

- For details regarding more conventional (non-CALEA) DNR equipment and DNR platforms, etc., go to the TICTU Website and consult the Traditional Technologies Intercept Team at [redacted]

  - **MANUALS:** For traditional DNR equipment Manuals see: [redacted]

In the past, there was little or no prospect of FISA Pen Register and Trap and Trace information ever being used in court or other public venues. However, based upon recent rulings of the Foreign Intelligence Surveillance Court (FISC) and new interpretations of the FISA law and its purposes by the Department of Justice, it is now conceivable that FISA-based Pen Register and Trap and Trace information could be used as evidence in criminal cases or otherwise made public. With respect to utilizing classified equipment, etc. in cases that may be prosecuted, the Department of Justice issued a directive in 2002 entitled: "Procedures for the Use of Classified Investigative Technologies in Criminal Cases." As a rule, these Procedures require coordination and clearance by the Department before such technologies can be used in criminal cases.

m) Evidence Acquisition/Recordation/Handling:

Pen Registers and Traps and Traces acquire dialed number as well as other call-control signaling information. Pen Register equipment used in local loop interceptions typically captures audio tones/signaling that is then portrayed as dialed numbers and/or other call-control indicators. Under CALEA, which is carrier (and principally switch)-based, the Pen Register and/or Trap and Trace information acquired is referred to as "call-identifying information (CII)." Under CALEA, delivery of CII to law enforcement is made over a "call data channel (CDC)." Details as to the elements/ format/messages for CALEA-compliant Pen Register and/or Trap and Trace uses in wireline and wireless networks are set forth in the J-STD-025.

The interface for collecting such Pen Register and/or Trap and Trace information may be DNR platforms such as those produced by JSI or the CALEA-related DCS-3000 platform, which may connected to the DCS-5000 (Red Wolf).

As noted, above, in the past, there was little prospect of FISA Pen Register and Trap and Trace information ever being used in court or other public venues. However, based upon recent rulings of the Foreign Intelligence Surveillance Court (FISC) and new interpretations of the FISA law and its purposes by the Department of Justice, it is now conceivable that FISA-based Pen Register and Trap and Trace information could be used as evidence in criminal cases or otherwise made public.

Once Pen Register and/or Trap and Trace information is acquired, the signaling information should be recorded electronically as the "original evidence." Electronic recordation can be accomplished through recorders attached to Pen Register/Trap and Trace DNR platforms such as those produced by JSI or the CALEA-related DCS-3000 platform or the DCS-5000 (Red Wolf).

Hardcopy printouts from the original electronic signaling may also constitute "original evidence." However, *post-processed* (manipulated) Pen/Trap printout information, such as that produced through the "Telephone Application (TA)," while user-friendly for investigators and prosecutors, is technically not original evidence because it has been processed/manipulated by the TA program.

If TTAs handle Pen Register/Trap evidence, they run the risk of becoming part of the "chain of custody" for the Pen/Trap evidence, thus exposing themselves to the possibility of having to testify (contrary to FBI policy). Hence, TTA involvement in evidence handling must be avoided.

- For details regarding the Facsimile Intercept Systems, go to the TICTU Website and consult the Traditional Technologies Intercept Team at [redacted]

· ***Switch-based:*** In implementing switch-based Title IIIs, TTAs frequently utilize the criminal law-based (JSI) DCS-6000 ("Voice Box") platform. The DCS 3000 system may also be used. In other conventional (non-CALEA) switch-based Title III, the interface for collecting such information may be one of the Pen Register DNR platforms produced by JSI.

- For details regarding the DCS-3000 system, go to the TICTU Website and consult the Switch-Based Intercept Team at [redacted]
- For details regarding the DCS-6000 system, go to the TICTU Website and consult the [redacted]
  - ➢ **MANUALS:** For details regarding major Title III collection platform Manuals see: [redacted]
- For details regarding more conventional (non-CALEA) Title III equipment and Title III platforms, etc., go to the TICTU Website and consult the Traditional Technologies Intercept Team at [redacted]
  - ➢ **MANUALS:** For details regarding traditional Title III equipment Manuals see: [redacted]

b2
b7E

· ***Network/Wireline Data-based:*** In implementing Network or Wireline Data-related Title IIIs, such Title IIIs are frequently implemented by service providers using their own proprietary or commercially-available equipment. In some cases, the FBI (DITU), or specially-trained TTAs, can also effect such Title IIIs utilizing tools commercially-available to law enforcement, such as [redacted]" Processing and viewing systems/tools such as [redacted] are also used.

- For details regarding the use of "products" such as [redacted] go to the DITU Website at [redacted]
  - ➢ **MANUALS:** For Manuals regarding products such as [redacted] go to the DITU Website at [redacted]

· ***High-Capacity -based:*** In implementing High-capacity-based Title IIIs or Pen Registers and/or Traps and Traces, such interceptions are frequently implemented by TTAs in concert with ATU personnel utilizing high-capacity access products such as those in the [redacted] suite, and the criminal law-based (JSI) DCS-6000 ("Voice Box") platform.

- For details regarding the [redacted] products, go to the ATU Website and consult the High-Capacity Access Team site at [redacted]
- For details regarding the DCS-6000 system, go to the TICTU Website and consult the [redacted]

techniques, equipment, and information from disclosure, TAs and TTAs should not needlessly disclose or display (or permit disclosure or display) of such material to FBI investigators, FBI personnel, or to others (to include USAs and Strike Force Attorneys).

Such nondisclosure pertains to details (including display) of this material. General descriptions or disclosures as to the overall technical functionality/operation of technical equipment or techniques are not prohibited. Any potential departure from this policy must be specifically approved by ITD at a unit chief or higher level before disclosure is made. See MIOG, Part 2, 10-10.13(4).

· ***FBI Testimony***: As set forth in MIOG, Part 2, 16-4.16, expert testimony regarding Title IIIs is available from the ITD. Such requests may emanate from Federal or State prosecutors or defense counsel. In a number of cases, such ITD personnel may be qualified to testify as subject matter experts in a given area within the Technical Investigative Program (TIP). In other cases, it would be more appropriate for non-FBI personnel (i.e., personnel from communication service providers, equipment manufacturers, software vendors, etc. to testify as experts in a given area of expertise.

The procedures for FBI technical personnel who testify as subject matter experts within the FBI's TIP are the same as those that apply to other FBI witnesses, including adherence to the dictates of 28 C.F.R.§ 16.21 et seq. Any legal or procedural questions should be promptly brought to the attention of the appropriate Assistant United States Attorney (AUSA) and the appropriate field office CDC or to an attorney in the Technology Law Unit, Office of the General Counsel, FBIHQ.

m) Evidence Acquisition/Recordation/Sealing/Handling:

· ***Evidence Acquisition***: Title III equipment, techniques, systems, and platforms acquire communications "content." Title III equipment used in local loop interceptions typically captures analog audio tones/signaling that is then captured as "content." Under CALEA, which is carrier and principally switch-based, Title III telephony content is referred to as call content and is transmitted over a "Call Content Channel (CCC)." Details as to the elements/format of CALEA-compliant call content in wireline and wireless networks are set forth in the J-STD-025. The interface for collecting call content may be DNR platforms such as those produced by JSI, or the CALEA-related DCS-3000 platform or the DCS-6000 (Voice Box) platform.

· ***Evidence Recordation***: Title III, at 18 U.S.C. 2518(8)(a), states that:

- the contents of any wire, oral, or electronic communication intercepted by any means authorized ... shall, if possible, be recorded on tape or wire or other comparable device.
- the recording of the contents of any wire, oral, or electronic communication ... shall be done in such way as will protect the recording from editing or other alterations...
- duplicate recordings may be made for use or disclosure ....
- custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing/denying judge and ... shall be kept for ten years.

Hence, once Title III content is acquired, the signaling information should be recorded electronically as the "original evidence." Such electronic recordation can be accomplished through

recorders attached to DNR platforms such as those produced by JSI or the CALEA-related DCS-3000 platform or the DCS-6000 (Voice Box) platform.

Hardcopy printouts from the original electronic signaling, such as email content, may also constitute "original evidence."

· ***Evidence Sealing:*** Title III, at 18 U.S.C. 2518(8)(a), states that:

- the presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom …
- immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions.

The U.S. Supreme Court has addressed the criticality of "sealing" recordings under Title III (18 U.S.C. 2518(8)(a)), with the potential for *exclusion* of the recorded evidence where delayed sealing occurs (even where no bad faith is found). *See United States v. Rios*, 495 U.S. 257 (1990).

Accordingly, FBI policy requires prompt "sealing" (and any necessary resealing) of recordings. MIOG, Part 2, 10-9.10(9) states:

> It is also necessary that the post-execution sealing requirements of Title 18, USC, Section 2518(8)(a) be met. Failure to adhere to this requirement could result in suppression of relevant interceptions in the absence of a satisfactory explanation for any delay in sealing. Agents should therefore be prepared to submit the original recordings of all interceptions to the issuing judicial official for sealing immediately at the conclusion of the period of continuously ordered electronic surveillance. In this context, if there is no break in time between the expiration of the original order and any subsequent extensions, Agents may wait until the expiration of the final extension before fulfilling this requirement.
>
> If any delay in making this delivery is anticipated, the Agent supervising the electronic surveillance should document the causes for this delay, i.e., duplication equipment failure, unforeseen manpower allocation priorities, and notify the supervising Assistant United States Attorney or Strike Force Attorney of the anticipated delay. If the supervising Agent anticipates this delay to be any greater than five days from the expiration date of the continuous electronic surveillance, he/she should, through the supervising attorney, within that five-day period obtain an extension of time in which to fulfill the sealing requirements from the appropriate judicial official.
>
> If original recordings require technical enhancement, analysis, comparisons, etc., the post-execution sealing requirement under Title 18, USC, Section 2518(8) still must be met. Therefore, procedurally, once the sealing requirement attaches, all recordings should be sealed in a timely fashion with the court first, and then unsealed with the court's approval if the recordings require enhancement, etc. Once unsealed, the recordings should be promptly submitted by the field to the Engineering Research Facility (ERF), Investigative Technology