Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION DOCUMENTS

Section: 34

Federal Bureau of Investigation
Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 21
Page 59 ~ b5, b6, b7C
Page 61 ~ b5
Page 62 ~ b5
Page 63 ~ b5
Page 64 ~ b5
Page 65 ~ b5, b6, b7C
Page 66 ~ b5, b6, b7C
Page 89 ~ b5, b6, b7C
Page 90 ~ b5
Page 91 ~ b5
Page 92 ~ b5
Page 93 ~ b5
Page 94 ~ b5, b6, b7C
Page 95 ~ b5, b6, b7C
Page 96 ~ b5, b6, b7C
Page 97 ~ b5, b6, b7C
Page 98 ~ b2, b5, b7E
Page 99 ~ b5
Page 100 ~ b5
Page 101 ~ b5
Page 102 ~ b5
DCS3000 is a pen register system that captures pertinent info from that side of the house. We are not concerned with it. Do not worry about the... That is run from headquarters and we can provide all the info on that. I don't know what DCS3000 is. Can you briefly explain it. Thanks.

Sorry to ask one of what I'm sure is a flood of questions about this, but...

The following databases are not listed in your message as one's covered by the "HQ team", nor were they listed in Dillingham's ec, do you know if these databases are subject to this tasking?:

DCS3000

Thanks, and sorry to pester you.
This is to clarify the requirements of the 12/20/2005 EC that was sent to all FBI divisions concerning FBI databases and a need to respond by January 13, 2006 with a description of such databases.

The EC requires descriptions of databases that are used in field offices but that are Bureau-wide, such as _____. We have decided that a more efficient manner of obtaining the same information is to have a single description of such databases, to include _____ and _____, circulated among the field offices. It will be drafted here at headquarters and Quantico. The field offices will simply need to state whether such descriptions are consistent with their particular operation and use of the database. If there are discrepancies, such discrepancies will have to be described. Hopefully, those descriptions will be circulated by the end of this week.

There does remain the issue of access to those databases, which is particular to individual field offices. Therefore, field offices still need to respond to questions 7 through 9 of the EC, which focus upon access to the databases, and question 20, which focuses upon the audit trail.

Further, the EC requires descriptions of all databases that are unique to the field offices. That requirement still stands, and all questions with respect to such databases (1 through 20) need to be answered.

CDCs- please disseminate this to those people in your field office who have responsibility for this project. Hopefully, this will eliminate a great deal of work on their part, but will still provide a clear and concise explanation of the databases, as well as any variations in operation or use that exist through the Bureau.

If anyone has any substantive questions concerning the responses, please contact OTD. For more general questions, feel free to contact me at (571) _____.

OGC/NSLB
Thanks, pik

---Original Message---

From: (AT) (FBI)
Sent: Thursday, February 09, 2006 8:18 AM
To: (OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

Asked one of the Tech Agents, and he said no.

---Original Message---

From: (AT) (FBI)
Sent: Thursday, February 09, 2006 8:13 AM
To: (OGC) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

The DCS-3000 have a more common or different name. I remember being told that but I can't think of what it was.

UNCLASSIFIED
The [9] 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 [9] and some of the other CALEA provided data), so I believe that it is being phased out.

Thanks. How about [9] or a system labeled simply as [9] (by Baltimore).-Original Message-

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 [9]).

DSC-3000 is the Collection system for pen data—to the extent it collects content it's limited to [9]—but it serves only as the collection point—the data is passed to another system (TA etc for analysis). PenLink appears to be a software application that can be used to help analyze pen data. (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 pen-link data can be imported into j2 Notebook.)
Anyone know what DCS-3000, Penlink (l-1) are. These are all new ones that are coming up in the course of reading field office responses.
From: (OGC) (FBI)  
Sent: Thursday, February 09, 2006 10:57 AM  
To: (OGC) (FBI)  
Subject: RE:  

UNCLASSIFIED  
NON-RECORD  

If you are able to access it is 319X-HQ-1487720, serial 86, the EC from Atlanta, it describes Thanks. 

--Original Message--  
From: (OGC) (FBI)  
Sent: Thursday, February 09, 2006 10:52 AM  
To: (OGC) (FBI)  
Subject: RE:  

UNCLASSIFIED  
NON-RECORD  

I couldn't find anything through Google on—do you have any more information that can point me to the right unit?? 

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

UNCLASSIFIED  
NON-RECORD  

Thanks. How about or a system labeled simply as (by Baltimore)_  

--Original Message--  
From: (OGC) (FBI)  
Sent: Thursday, February 09, 2006 8:48 AM  
To: (OGC) (FBI)  
Cc: (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 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.
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 pen-link data can be imported into i2 Notebook.)

UNCLASSIFIED
NON-RECORD

Anyone know what DCS-3000, Penlink(I-1) are. These are all new ones that are coming up in the course of reading field office responses.
I was forwarded your email by Mobile ASAC Bill Lewis regarding our FISA collection/processing systems.

Following are the access list(s) for Pen Register systems (Both DCS 3000 and Wireline) both contain Pen Register data.

DCS 3000 and Wireline

TA Systems Administrator
TTA - Has been granted administrative privileges
TTA - Has been granted administrative privileges
Elser Technician - Performs daily downloads of collected data for transfer to case agent

TA Systems Administrator
TTA - Has been granted administrative privileges
TTA - Has been granted administrative privileges
BAE Contracto (Retired TTA)- Has been granted administrative privileges for software and firmware upgrades.

Please note that the CSOC at Quantico has been granted remote access to the system for health maintenance and to insure that this system remains operational during off hours.

Also note that we have an access point to the Mobile and have the ability to route FISA audio to Language Services Division. To date we have not passed any audio through this system and have not used EDMS. Should you need any additional information, I can be reached at the following telephone numbers...Steve
Thanks. From my point of view, it means NO MORE DESCRIPTIONS NEED TO BE ADDED from that list, at least.

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

UNCLASSIFIED NON-RECORD

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.

-----Original Message-----
From: OGC (FBI) 
Sent: Wednesday, February 15, 2006 11:04 AM 
To: 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
Attached please find electronic copies of the Privacy Threshold Analysis (PTA) forms for the four (4) Operational Technology Division systems identified as part of the twenty-eight (28) law enforcement systems on the FBI's 2006 FISMA inventory; specifically the Data Collection System 3000 (DCS-3000), the Field Office Integrated Security System, the Computer Analysis Response Team Storage Area Network (CART SAN) and the Forensic Audio, Video and Image Analysis Unit Local Area Network (FAVIAU LAN). These are being forwarded to you per the June 5, 2006 e-mail attached below which requested they be forwarded to you "NLT" 6/9/06 (which was determined to mean "by close of business" 6/9/06 pursuant to a telephone conversation with OGC's"

PTADC3000.wpd PTAFQ1SS.wpd PTACARTSAN.wpd PTAFAVIAU.wpd
(57 KB) (57 KB) (62 KB) (55 KB)

The original copies of the PTAs concerning the DCS-3000 and the Field Office Integrated Security System where sent to your attention today via Bureau mail. It is my understanding that pursuant to telephone conversations between the POCs for the CART SAN and FAVIAU LAN systems and OGC via Bureau mail, the original copies for those two PTAs where sent directly to Ms.

Should you have any questions regarding this matter please don't hesitate to contact me. Thanks

SSA
Assistant Section Chief
Technical Programs Section
Operational Technology Division

—Original Message—
From: OGC (FBI) On Behalf Of CAPRONI, VALERIE E. (OGC (FBI)
Sent: Monday, June 05, 2006 3:50 PM
To: FBI ADs and EADs
Subject: Urgent request-DAG short-fused PIA tasking
I very much need your assistance to meet a short-fused, very high-visibility DAG tasking that the FBI received yesterday. The tasking relates to requirements by DOJ (passing down requirements by OMB) that agencies must on a quarterly basis certify 90% completion (for all FBI systems) of Privacy Impact Assessments (PIAs) required by Section 208 of the E-Government Act (E-Gov). To meet the two deadlines imposed by DOJ, we will need completed inputs by affected divisions by 6/9 and 6/21, as described below.

The FBI has been doing our own PIAs for years, and we have known about the changes looming under E-Gov for many months. Indeed, many of you probably have already encountered the effects in your own programs, such as increased emphasis on PIAs appearing in procurement/IT management processes, and DD Pistole's EC of 5/15/06 (BUDED 6/5/2006) requiring each division to appoint a division privacy contact. We have, however, been long awaiting specific implementation guidance from DOJ, resolution of which was only recently provided thanks to the recent arrival of DOJ's new Chief Privacy and Civil Liberties Officer (Jane Horvath). This culminated in the 5/30/2006 DAG memo which we received yesterday (TRIM 06/DO/3020) directing the FBI to focus on the 28 FBI Law Enforcement systems on the FBI's 2006 FISMA inventory (see attached).

The FBI must complete a Privacy Threshold Analysis (PTA) for each system and, where so indicated by the PTA, we must also complete at least a short-form PIA.

OGC is responsible for coordinating the PIA process, and yesterday to meet this emergent requirement I directed internal detailing of OGC personnel to double our PIA-processing cadre, which will work exclusively on this tasking through completion.

But I can't emphasize strongly enough that PIA completion also depends on the absolutely essential contributions of knowledgeable program management in fully describing a system's structure, capabilities, and operations. Successful PIA completion thus must always entail a collaborative effort with program management (which may span several divisions, e.g., the system builder(s) and its end user(s)), and it is to this end that I ask you to direct and support the provision of priority assistance from your affected system sponsors, project officers, and other personnel as may be required to complete this tasking within DOJ's deadlines.

To do this, we need divisions to complete PTAs for their systems NLT next Friday (6/9) and complete any required short-form PIAs NLT Wednesday 6/21.
Unfortunately, the DOJ tasking also appears to require that we use newly implemented DOJ forms (attached for your reference are PTA and short-PIA forms):

(Privacy Threshold privacy_impact_assessment)

(The long PIA form is here:

Completion guidance is here:

Plus we need to submit the completed forms to DOJ for approval, which will require some departures from previous FBI SOP, and perhaps (and more irritatively) some rewriting of previous drafts. (Hopefully, however, any previously prepared materials you may have prepared will prove susceptible to cutting/pasting into the new forms. And who knows, it may even be that, once the initial kinks are worked out, the new PIA process might even help make it easier and/or faster to complete and process PIAs, which would be nice, because there surely are more PIAs in all our futures.)

By separate e-mails, OGC's PIA staff will be communicating directly with the persons identified as POCs for each of the 28 FBI systems affected by this tasking. We will provide the division program POCs with the necessary forms for the program to complete (plus some additional questions we need for our review), and we will identify a designated OGC attorney to be OGC's POC for each system who will work with the division POCs to "smooth" the form(s) within the deadline(s).

My overall coordinator for this tasking is Senior Assistant General Counsel _______ 202-324 _______ (Note there are now 3 in the FBI internal e-mail address is the only one in OGC), and his Internet e-mail address is: _______. Please don't hesitate to contact my Deputy Pat Kelley (202-324-_____) or me (202-324-_____) you have any questions. Thanks in advance for your support!

VC

UNCLASSIFIED
PTADCS3000.wpd
(57 KB)
DCS3000 application suite was developed to assist law enforcement agencies (LEAs) with collecting and processing data for court-ordered electronic surveillance (ELSUR) operations. LEAs dial into switches, which are devices used by telecommunications service providers to route telephone calls to their destinations. The DCS3000 can collect ELSUR data under the following warrant types: Pen Register (deals with call data), and Title III (deals with call data and content). The DCS3000 collects data from the Telecommunications Service Provider (TSP) and stores it at the LEA site. The TSP provides Call Data Channel (CDC) data. The data first flows through the VanGuard, which stores it until requested by the Multiserver, which then forwards the data to the Client, where the CDC data is stored.
From: OGC (FBI)
Sent: Friday, June 09, 2006 4:00 PM
To: OGC (FBI)
Cc: THOMAS, MARCUS C. (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI)
Subject: RE: Urgent request-DAG short-fused PIA tasking

P.S. The FBI is now blessed with three. And one is also. I'm the one in OGC.
Attached please find electronic copies of the Privacy Threshold Analysis (PTA) forms for the four (4) Operational Technology Division systems identified as part of the twenty-eight (28) law enforcement systems on the FBI's 2006 FISMA inventory; specifically the Data Collection System 3000 (DCS-3000), the Field Office Integrated Security System, the Computer Analysis Response Team Storage Area Network (CART SAN) and the Forensic Audio, Video and Image Analysis Unit Local Area Network (FAVIAU LAN). These are being forwarded to you per the June 5, 2006 e-mail attached below which requested they be forwarded to you "NLT" 6/9/06 (which was determined to mean "by close of business" 6/9/06 pursuant to a telephone conversation with OGC's [ ]

The original copies of the PTAs concerning the DCS-3000 and the Field Office Integrated Security System where sent to your attention today via Bumail. It is my understanding that pursuant to telephone conversations between the POCs for the CART SAN and FAVIAU LAN systems and OGC's [ ] the original copies for those two PTAs where sent directly to Ms [ ] via Bureau mail.

Should you have any questions regarding this matter please don't hesitate to contact me. Thanks

SSA]

Assistant Section Chief
Technical Programs Section
Operational Technology Division

Original Message

From: [ ] (OGC (FBI) On Behalf Of CAPRONI, VALERIE E. (OGC (FBI)
Sent: Monday, June 5, 2006 3:53 PM
To: FBI_ADs and EADs
Subject: Urgent request-DAG short-fused PIA tasking
Importance: High

I very much need your assistance to meet a short-fused, very high-visibility DAG tasking that the FBI received yesterday. The tasking relates to requirements by DOJ (passing down requirements by OMB) that agencies must on a quarterly basis certify 90% completion (for all FBI systems) of Privacy Impact Assessments (PIAs) required by Section 208 of the
E-Government Act (E-Gov). To meet the two deadlines imposed by DOJ, we will need completed inputs by affected divisions by 6/9 and 6/21, as described below.

The FBI has been doing our own PIAs for years, and we have known about the changes looming under E-Gov for many months. Indeed, many of you probably have already encountered the effects in your own programs, such as increased emphasis on PIAs appearing in procurement/IT management processes, and DD Pistole’s EC of 5/15/06 (BUDED 6/5/2006) requiring each division to appoint a division privacy contact. We have, however, been long awaiting specific implementation guidance from DOJ, resolution of which was only recently provided thanks to the recent arrival of DOJ’s new Chief Privacy and Civil Liberties Officer (Jane Horvath). This culminated in the 5/30/2006 DAG memo which we received yesterday (TRIM 06/DO/3020) directing the FBI to focus on the 28 FBI Law Enforcement systems on the FBI’s 2006 FISMA inventory (see attached).

The FBI must complete a Privacy Threshold Analysis (PTA) for each system and, where so indicated by the PTA, we must also complete at least a short-form PIA.

OGC is responsible for coordinating the PIA process, and yesterday to meet this emergent requirement I directed internal detailing of OGC personnel to double our PIA-processing cadre, which will work exclusively on this tasking through completion.

But I can’t emphasize strongly enough that PIA completion also depends on the absolutely essential contributions of knowledgeable program management in fully describing a system’s structure, capabilities, and operations. Successful PIA completion thus must always entail a collaborative effort with program management (which may span several divisions, e.g., the system builder(s) and its end user(s)), and it is to this end that I ask you to direct and support the provision of priority assistance from your affected system sponsors, project officers, and other personnel as may be required to complete this tasking within DOJ’s deadlines.

To do this, we need divisions to complete PTAs for their systems NLT next Friday (6/9) and complete any required short-form PIAs NLT Wednesday 6/21.

Unfortunately, the DOJ tasking also appears to require that we use newly implemented DOJ forms (attached for your reference are PTA and short-PIA forms):

(The long PIA form is here: privacy_impact_assessment_short_form_template_90_cert.doc)

Plus we need to submit the completed forms to DOJ for approval, which will require some departures from previous FBI SOP, and perhaps (and more irritatingly) some rewriting of previous drafts. (Hopefully, however, any previously prepared materials you may have
prepared will prove susceptible to cutting/pasting into the new forms. And who knows, it may even be that, once the initial kinks are worked out, the new PIA process might even help make it easier and/or faster to complete and process PIAs, which would be nice, because there surely are more PIAs is all our futures.)

By separate e-mails, OGC's PIA staff will be communicating directly with the persons identified as POCs for each of the 28 FBI systems affected by this tasking. We will provide the division program POCs with the necessary forms for the program to complete (plus some additional questions we need for our review), and we will identify a designated OGC attorney to be OGC's POC for each system who will work with the division POCs to "smooth" the form(s) within the deadline(s).

My overall coordinator for this tasking is Senior Assistant General Counsel [Name]. (Note there are now 3 internal e-mail addresses in the FBI, the only one in OGC), and his Internet e-mail address is [Name]. Please don't hesitate to contact my Deputy Pat Kelley (202-324 [Name]), or me (202-324 [Name]) if you have any questions. Thanks in advance for your support!

VC
<table>
<thead>
<tr>
<th>FY08-030</th>
<th>FY08-031 SMIS</th>
<th>Completed 10/10/05</th>
<th>Need to publish</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FY08-032 FBI Digital Collection</strong>&lt;br&gt;(DCS-3000, DCS-5000 and DCS-6000)</td>
<td>N/NSS</td>
<td>Collects audio, microphone, and fax intercepts. A PIA is not required pursuant to the E-Government Act because the FBI's Digital Collection Systems are considered national security systems. However, the FBI conducts internal PIAs on all national security systems to ensure that privacy rights are adequately considered in system development. A PIA was conducted and approved 8/27/2001 for the digital collection systems. OTD performed an upgrade to the system in July of 2005. By EC dated 12/22/2005, OGC advised that a supplemental PIA was not required, and that OGC should be consulted for any subsequent upgrades.</td>
<td></td>
</tr>
<tr>
<td><strong>FY08-033 Administrative Systems Support</strong></td>
<td>Yes, unless it is a NSS</td>
<td>Required. Possibly covered by existing but may need update</td>
<td>Will contain, among other things, BPMS &amp; Personnel Background Mgmt System, both of which would contain personal info.</td>
</tr>
<tr>
<td>FY08-034</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY08-035</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FY08-036 Network Services</strong></td>
<td>N/NSS</td>
<td>Required. Exists but may need update</td>
<td>NSS (according to hart)</td>
</tr>
<tr>
<td><strong>FY08-037 Records Management Application</strong></td>
<td>N/NSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FY08-038 Operations Test and Evaluation Facility</strong></td>
<td>Not required</td>
<td>Not required</td>
<td>As presented in the Exhibit 300, this investment will provide the FBI with an environment isolated from but representative of the FBI operational environment, for the conduct of independent verification and validation of all new or enhanced IT systems to be used within the FBI. No PIA is required for the establishment of OTEF, since of itself the OTEF is merely a testing environment that does not per se constitute a personal information system or collection; indeed we would anticipate that many of the actual tests conducted would not involve personally identifiable information, e.g., if the tests merely involved technical stressing of an application or dummy data. (Note, though, that acquisition of the functionality being tested might require a PIA by the acquisition sponsor.) PIAs might be required for specific OTEF tests if the testing entailed OTEF's access to non-minor amounts of personally identifiable real data. (But even in such cases, it may be the most pragmatic solution would be to satisfy any PIA requirements by addressing OTEF testing in the underlying PIA for the system or procurement being tested.)</td>
</tr>
<tr>
<td>FY08-040</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From: (OGC) (FBI)
Sent: Friday, June 09, 2006 12:30 PM
To: THOMAS, MARCUS C. (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI)
Cc: (OGC) (FBI); (OTD) (OGA); (ITD) (FBI) (OTD)
Subject: RE: Urgent request-DAG short-fused PIA tasking

UNCLASSIFIED NON-RECORD

My contacts for CARTSAN and the Forensic Audio, Video and Image Analysis Unit Local Area Network were [insert names]. Both were superb in their efforts to assist me with this project. Many thanks to all.

Sincerely,

[Signature]

Assistant General Counsel
Administrative Law Unit, Room 7338
202-324

THIS IS A PRIVILEGED COMMUNICATION AND IS NOT TO BE DISTRIBUTED WITHOUT PRIOR OGC APPROVAL

Attached please find electronic copies of the Privacy Threshold Analysis (PTA) forms for the four (4) Operational Technology Division systems identified as part of the twenty-eight (28) law enforcement systems on the FBI's 2006 FISMA inventory: specifically the Data Collection System 3000 (DCS-3000), the Field Office Integrated Security System, the Computer Analysis Response Team Storage Area Network (CART SAN) and the Forensic Audio, Video and Image Analysis Unit Local Area Network (FAVIAU LAN). These are being forwarded to you per the June 5, 2006 e-mail attached below which requested they be forwarded to you "NLT" 6/9/06 (which was determined to mean "by close of business" 6/9/06 pursuant to a telephone conversation with OGC).

<< File: PTADCS3000.wpd >> << File: PTAFOISS.wpd >> << File: PTACARTSAN.wpd >>
The original copies of the PTAs concerning the DCS-3000 and the Field Office Integrated Security System were sent to your attention today via Bumail. It is my understanding that pursuant to telephone conversations between the POCs for the CART SAN and FAVIAU LAN systems and OGC: the original copies for those two PTAs were sent directly to [redacted] via Bureau mail.

Should you have any questions regarding this matter please don't hesitate to contact me.

Thanks

[Redacted]

Assistant Section Chief
Technical Programs Section
Operational Technology Division
(703) 634

---Original Message---

From: [Redacted] (FBI) On Behalf Of CAPRONI, VALERIE E. (OGC) (FBI)
Sent: Monday, June 05, 2006 3:50 PM
To: [Redacted], FBI ADs and EADs
Subject: Urgent request-DAG short-fused PIA tasking
Importance: High

UNCLASSIFIED
NON-RECORD

I very much need your assistance to meet a short-fused, very high-visibility DAG tasking that the FBI received yesterday. The tasking relates to requirements by DOJ (passing down requirements by OMB) that agencies must on a quarterly basis certify 90% completion (for all FBI systems) of Privacy Impact Assessments (PIAs) required by Section 208 of the E-Government Act (E-Gov). To meet the two deadlines imposed by DOJ, we will need completed inputs by affected divisions by 6/9 and 6/21, as described below.

The FBI has been doing our own PIAs for years, and we have known about the changes looming under E-Gov for many months. Indeed, many of you probably have already encountered the effects in your own programs, such as increased emphasis on PIAs appearing in procurement/IT management processes, and DD Pistole's EC of 5/15/06 (BUDED 6/5/2006) requiring each division to appoint a division privacy contact. We have, however, been long awaiting specific implementation guidance from DOJ, resolution of which was only recently provided thanks to the recent arrival of DOJ's new Chief Privacy and Civil Liberties Officer (Jane Horvath). This culminated in the 5/30/2006 DAG memo which we received yesterday (TRIM 06/DO/3020) directing the FBI to focus on the 28 FBI Law Enforcement systems on
the FBI's 2006 FISMA inventory (see attached).

The FBI must complete a Privacy Threshold Analysis (PTA) for each system and, where so indicated by the PTA, we must also complete at least a short-form PIA.

OGC is responsible for coordinating the PIA process, and yesterday to meet this emergent requirement I directed internal detailing of OGC personnel to double our PIA-processing cadre, which will work exclusively on this tasking through completion.

But I can't emphasize strongly enough that PIA completion also depends on the absolutely essential contributions of knowledgeable program management in fully describing a system's structure, capabilities, and operations. Successful PIA completion thus must always entail a collaborative effort with program management (which may span several divisions, e.g., the system builder(s) and its end user(s)), and it is to this end that I ask you to direct and support the provision of priority assistance from your affected system sponsors, project officers, and other personnel as may be required to complete this tasking within DOJ's deadlines.

To do this, we need divisions to complete PTAs for their systems NLT next Friday (6/9) and complete any required short-form PIAs NLT Wednesday 6/21.

Unfortunately, the DOJ tasking also appears to require that we use newly implemented DOJ forms (attached for your reference are PTA and short-PIA forms):

Plus we need to submit the completed forms to DOJ for approval, which will require some departures from previous FBI SOP, and perhaps (and more irritatingly) some rewriting of previous drafts. (Hopefully, however, any previously prepared materials you may have prepared will prove susceptible to cutting/pasting into the new forms. And who knows, it may even be that, once the initial kinks are worked out, the new PIA process might even help make it easier and/or faster to complete and process PIAs, which would be nice, because there surely are more PIAs is all our futures.)

By separate e-mails, OGC's PIA staff will be communicating directly with the persons identified as POCs for each of the 28 FBI systems affected by this tasking. We will provide the division program POCs with the necessary forms for the program to complete (plus some additional questions we need for our review), and we will identify a designated OGC attorney to be OGC's POC for each system who will work
with the division POCs to "smooth" the form(s) within the deadline(s).

My overall coordinator for this tasking is Senior Assistant General Counsel 202-324-XXX (Note: there are now two in the FB) internal email address is the only one in OGC), and his Internet e-mail address is XXX. Please don't hesitate to contact me if you have any questions.

Deputy Pat Kelley (202-324-XXX) or me (202-324-XXX) if you have any questions.

Thanks in advance for your support!

VC
From: (OTD) (FBI)
Sent: Friday, June 09, 2006 4:30 PM
To: (OGC) (FBI); (OGC) (FBI);
Cc: THOMAS, MARCUS C. (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI)
Subject: RE: Urgent request-DAG short-fused PIA tasking

UNCLASSIFIED
NON-RECORD

Thank you very much! After the dust settles, let me know what you want us to do and it will be handled.

Have a great weekend.

FYI - Please, note comments regarding the PTA for the CARTSAN. I'll keep you posted.

SSA
Assistant Section Chief
Technical Programs Section
Operational Technology Division
(703) 63

Original Message
From: (OGC) (FBI)
Sent: Friday, June 09, 2006 4:00 PM
To: (FBI)
Cc: THOMAS, MARCUS C. (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); CLIFFORD, MICHAEL (OTD) (FBI)
Subject: RE: Urgent request-DAG short-fused PIA tasking

UNCLASSIFIED
NON-RECORD
P.S. The FBI is now blessed with three (and one is also) in OGC.

----- Original Message -----
From: THOMAS, MARCUS C (OTD) (FBI)
Sent: Friday, June 09, 2006 10:40 AM
To: CLIFFORD, MICHAEL (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD); (OGC) (FBI); OGC (FBI)
Cc: THOMAS, MARCUS C (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD)
Subject: FW: Urgent request-DAG short-fused PIA tasking
Importance: High

UNCLASSIFIED
NON-RECORD

Attached please find electronic copies of the Privacy Threshold Analysis (PTA) forms for the four (4) Operational Technology Division systems identified as part of the twenty-eight (28) law enforcement systems on the FBI's 2006 FISMA inventory; specifically the Data Collection System 3000 (DCS-3000), the Field Office Integrated Security System, the Computer Analysis Response Team Storage Area Network (CART SAN) and the Forensic Audio, Video and Image Analysis Unit Local Area Network (FAVIAU LAN). These are being forwarded to you per the June 5, 2006 e-mail attached below which requested they be forwarded to you "NLT" 6/9/06 (which was determine to mean "by close of business" 6/9/06 pursuant to a telephone conversation with OGC)

<< File: PTADCS3000.wpd >> << File: PTAFOISS.wpd >> << File: PTACARTSAN.wpd >>
<< File: PTAFAVIAU.wpd >>
The original copies of the PTAs concerning the DCS-3000 and the Field Office Integrated...
Security System where sent to your attention today via Bumail. It is my understanding that pursuant to telephone conversations between the POCs for the CART SAN and FAVIAU LAN systems and OGC's, the original copies for those two PTAs where sent directly to you via Bureau mail.

Should you have any questions regarding this matter please don't hesitate to contact me.

Thanks

[Signature]

Assistant Section Chief
Technical Programs Section
Operational Technology Division

---Original Message---

From: OGC (FBI) On Behalf Of CAPRONI, VALERIE E. (OGC) (FBI)
Sent: Monday, June 05, 2006 3:50 PM
To: FBI AIDs and EADs
Subject: Urgent request-DAG short-fused PIA tasking
Importance: High

UNCLASSIFIED
NON-RECORD

I very much need your assistance to meet a short-fused, very high-visibility DAG tasking that the FBI received yesterday. The tasking relates to requirements by DOJ (passing down requirements by OMB) that agencies must on a quarterly basis certify 90% completion (for all FBI systems) of Privacy Impact Assessments (PIAs) required by Section 208 of the E-Government Act (E-Gov). To meet the two deadlines imposed by DOJ, we will need completed inputs by affected divisions by 6/9 and 6/21, as described below.

The FBI has been doing our own PIAs for years, and we have known about the changes looming under E-Gov for many months. Indeed, many of you probably have already encountered the effects in your own programs, such as increased emphasis on PIAs appearing in procurement/IT management processes, and DD Pistole's EC of 5/15/06 (BUDED 6/5/2006) requiring each division to appoint a division privacy contact. We have, however, been long awaiting specific implementation guidance from DOJ, resolution of which was only recently provided thanks to the recent arrival of DOJ's new Chief Privacy and Civil Liberties Officer (Jane Horvath). This culminated in the 5/30/2006 DAG memo which we received yesterday (TRIM 06/DO/3020) directing the FBI to focus on the 28 FBI Law Enforcement systems on the FBI's 2006 FISMA inventory (see attached).

<< File: FISMA_LE_Spreadsheet (version 2) from Susan 5-30-06.xls >>

The FBI must complete a Privacy Threshold Analysis (PTA) for each system and,
where so indicated by the PTA, we must also complete at least a short-form PIA.

OGC is responsible for coordinating the PIA process, and yesterday to meet this emergent requirement I directed internal detailing of OGC personnel to double our PIA-processing cadre, which will work exclusively on this tasking through completion.

But I can't emphasize strongly enough that PIA completion also depends on the absolutely essential contributions of knowledgeable program management in fully describing a system's structure, capabilities, and operations. Successful PIA completion thus must always entail a collaborative effort with program management (which may span several divisions, e.g., the system builder(s) and its end user(s)), and it is to this end that I ask you to direct and support the provision of priority assistance from your affected system sponsors, project officers, and other personnel as may be required to complete this tasking within DOJ's deadlines.

To do this, we need divisions to complete PTAs for their systems NLT next Friday (6/9) and complete any required short-form PIAs NLT Wednesday 6/21.

Unfortunately, the DOJ tasking also appears to require that we use newly implemented DOJ forms (attached for your reference are PTA and short-PIA forms):

[Files: Privacy Threshold Analysis.Short.Form.PIA.wpd, Privacy_impact_assessment_short form template_90 cert.doc]

(The long PIA form is here:)

[Completion guidance is here:]

Plus we need to submit the completed forms to DOJ for approval, which will require some departures from previous FBI SOP, and perhaps (and more irritatingly) some rewriting of previous drafts. (Hopefully, however, any previously prepared materials you may have prepared will prove susceptible to cutting/pasting into the new forms. And who knows, it may even be that, once the initial kinks are worked out, the new PIA process might even help make it easier and/or faster to complete and process PIAs, which would be nice, because there surely are more PIAs is all our futures.)

By separate e-mails, OGC's PIA staff will be communicating directly with the persons identified as POCs for each of the 28 FBI systems affected by this tasking. We will provide the division program POCs with the necessary forms for the program to complete (plus some additional questions we need for our review), and we will identify a designated OGC attorney to be OGC's POC for each system who will work with the division POCs to "smooth" the form(s) within the deadline(s).

My overall coordinator for this tasking is Senior Assistant General Counsel [202-324] (Note there are now [ ] in the FBI).
internal e-mail address is [REDACTED] (the only one in OGC), and his Internet e-mail address is [REDACTED]. Please don't hesitate to contact [REDACTED] my Deputy Pat Kelley (202-324 [REDACTED]) or me (202-324 [REDACTED]) if you have any questions. Thanks in advance for your support!

VC
<table>
<thead>
<tr>
<th>System Name</th>
<th>PTA</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Campus WAN</td>
<td>Campus WAN</td>
</tr>
<tr>
<td>4 Chemical Network (ChemNet)</td>
<td>ChemNet</td>
</tr>
<tr>
<td>5 CJIS WAN</td>
<td>CJIS WAN</td>
</tr>
<tr>
<td>6 Combined DNA Index System (CODIS)</td>
<td>N/A (PIA previously conducted)</td>
</tr>
<tr>
<td>7 Commercial Payments Unit Invoice Management System (CPUIMS)</td>
<td>CPUIMS</td>
</tr>
<tr>
<td>8 Computer Analysis Response Storage Area Network, (CARTSAN)</td>
<td>CARTSAN</td>
</tr>
<tr>
<td>9 CYBERTRANS II</td>
<td>CYBERTRANS II</td>
</tr>
<tr>
<td>10 Data Collection System 3000 (DCS-3000)</td>
<td>DCS-3000</td>
</tr>
<tr>
<td>11 Digital Document Management System (DDMS)</td>
<td>DDMS</td>
</tr>
<tr>
<td>12 Document Capture System</td>
<td>Document Capture System</td>
</tr>
<tr>
<td>13 Financial Management System (FMS)</td>
<td>FMS</td>
</tr>
<tr>
<td>14 Field Office Integrity Security System (FOISS)</td>
<td>FOISS</td>
</tr>
<tr>
<td>15 Forensic Audio, Video, and Image Analysis (FAVIA) LAN</td>
<td>FAVIA LAN</td>
</tr>
<tr>
<td>16 Innocent Images Case Management System (IICMS)</td>
<td>N/A (PIA previously conducted)</td>
</tr>
<tr>
<td>17 Integrated Automated Fingerprint Identification System (IAFIS)</td>
<td>3 PTAs:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1) interim Data Sharing Model (iDSM)</td>
</tr>
<tr>
<td></td>
<td>(2) Composite PTA for following future components of Next Generation IAFIS (NGI):</td>
</tr>
<tr>
<td></td>
<td>Enhanced IAFIS Repository;</td>
</tr>
<tr>
<td></td>
<td>Advanced Fingerprint Identification Technology (AFIT)</td>
</tr>
<tr>
<td></td>
<td>(including the Enhanced Terrorist Identification Service (ETIS));</td>
</tr>
<tr>
<td></td>
<td>National Palm Print System (NPPS);</td>
</tr>
<tr>
<td></td>
<td>National Security Interest File (NSIF); and</td>
</tr>
<tr>
<td></td>
<td>Interstate Photo System (IPS)</td>
</tr>
<tr>
<td></td>
<td>(3) Current national security enhancements</td>
</tr>
<tr>
<td>18 Law Enforcement Online (LEO)</td>
<td>LEO</td>
</tr>
<tr>
<td>19 National Crime Information Center (NCIC)</td>
<td>Violent Gang and Terrorist Organization File (VGTOF)</td>
</tr>
</tbody>
</table>
Hope this provides what you need. If not, please let me know. If you need a more succinct or technical description, I’ll provide it.

Glad we finally met. Thanks for your help.

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. Digital Collection supports the FBI’s mission to ensure the ability of the FBI to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems being acquired under the Digital Collection program include systems (foreign counterintelligence and law enforcement) that possess similar functions and capabilities to intercept telephone, microphone, and facsimile communications; however, the primary difference is law enforcement system’s requirement to minimize collected communications. The passage of the Communication Assistance to Law Enforcement Act (CALEA), the implementation of state-of-the-art personal security features, and the explosion of telecommunication options (caller ID, call waiting, call conferencing, etc.) spotlighted the deficiencies of the legacy systems.

The Digital Collection Program provides the FBI with the means to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems which facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems provided through this program intercept multi-source digital (and analog) communications information for intelligence gathering for foreign counterintelligence activities and investigative purposes for providing evidence of criminal activity for trial. It should be noted that those systems used for criminal investigations possess a requirement to minimize intercepted voice sessions, i.e., record only when the call is being actively monitored. Electronic information collected includes pen register (incoming and outgoing dialed digits, caller identification, date/time of communication, and other signal related information), analog and digital telephone calls, facsimile and modem transmissions, and microphone audio. High density drives and magneto-optical disks are utilized for temporary and permanent storage, respectively; no special, environmental storage facilities are needed. Digital Collection systems are used primarily by FBI field offices and Resident Agencies in support of active foreign intelligence and criminal cases. Support is also provided to other federal, state, local and tribal agencies, as required.

The Digital Collection Program has evolved during its life cycle and has become more complex. Even so, digital collection systems are computer-based systems comprised primarily of commercial-off-the-shelf hardware and software with limited proprietary application software. Incorporated technological advances allow Case Agents to easily and effectively manage the recordings electronically, which dramatically increases the efficiency of trial preparations. While each Field Office or Resident Agency is self-sustaining in its ability to process intercepted information, this program permits interconnectivity of all FCI systems via a wide area network established to link field offices’ central monitoring plants for the purpose of digital collection information sharing; it will use Trilogy’s network backbone.) and TRILOGY (the FBI’s enterprise wide area network being deployed to link field offices). This connectivity enables the transfer of electronic or digital files of intercepts to a remote or distant field office for special language translation/transcription and sharing of information among FBI offices and other partnering agencies. Systems are also installed as fixed systems in locations that require long-term, permanent operations. In many instances, intercepted audio is shared via a secure, wide area network or downloaded from computer memory onto removable media and provided to language specialists in offices around the country, greatly increasing productivity of FBI translation and transcription efforts.
productivity of FBI translation and transcription efforts.
Subject: Digital Collection description

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. Digital Collection supports the FBI's mission to ensure the ability of the FBI to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems being acquired under the Digital Collection program include systems (foreign counterintelligence and law enforcement) that possess similar functions and capabilities to intercept telephone, microphone, and facsimile communications; however, the primary difference is law enforcement system's requirement to minimize collected communications. The passage of the Communication Assistance to Law Enforcement Act (CALEA), the implementation of state-of-the-art personal security features, and the explosion of telecommunication options (caller ID, call waiting, call conferencing, etc.) spotlighted the deficiencies of the legacy systems.

The Digital Collection Program provides the FBI with the means to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems which facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems provided through this program intercept multi-source digital (and analog) communications information for intelligence gathering for foreign counterintelligence activities and investigative purposes for providing evidence of criminal activity for trial. It should be noted that those systems used for criminal investigations possess a requirement to minimize intercepted voice sessions. (i.e., record only when the call is being actively monitored). Electronic information collected includes pen register (incoming and outgoing dialed digits, caller identification, date/time of communication, and other signal related information), analog and digital telephone calls, facsimile and modem transmissions, and microphone audio. High density drives and magneto-optical disks are utilized for temporary and permanent storage, respectively; no special, environmental storage facilities are needed. Digital collection systems are used primarily by FBI field offices and Resident Agencies in support of active foreign intelligence and criminal cases. Support is also provided to other federal, state, local and tribal agencies, as required.

The Digital Collection Program has evolved during its life cycle and has become more complex. Even so, digital collection systems are computer-based systems comprised primarily of commercial-off-the-shelf hardware and software with limited proprietary application software. Incorporated technological advances allow case Agents to easily and effectively manage the recordings electronically, which dramatically increases the efficiency of trial preparations. While each Field Office or Resident
Agency is self-sustaining in its ability to process intercepted information, this program permits interconnectivity of all FCI systems via a wide area network established to link field offices' central monitoring plants for the purpose of digital collection information sharing; it will use Trilogy's network backbone.) and TRILOGY (the FBI's enterprise wide area network being deployed to link field offices). This connectivity enables the transfer of electronic or digital files of intercepts to a remote or distant field office for special language translation/transcription and sharing of information among FBI offices and other partnering agencies. Systems are also installed as fixed systems in locations that require long-term, permanent operations. In many instances, intercepted audio is shared via a secure, wide area network or downloaded from computer memory onto removable media and provided to language specialists in offices around the country, greatly increasing productivity of FBI translation and transcription efforts.

UNCLASSIFIED

UNCLASSIFIED

From: FT ED (OTD) (CON)
Sent: Friday, November 04, 2005 7:47 AM
To: GGC (FBI)
Cc: OTD (FBI)
Subject: Digital Collection description

UNCLASSIFIED

NON-RECORD

-Hope this provides what you need. If not, please let me know. If you need a more succinct or technical description, I'll provide it.

Glad we finally met. Thanks for your help.

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. Digital Collection supports the FBI's mission to ensure the ability of the FBI to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems being acquired under the Digital Collection program include systems (foreign counterintelligence and law enforcement) that possess similar functions and capabilities to intercept telephone, microphone, and facsimile communications; however, the primary difference is law enforcement system's requirement to minimize collected communications. The passage of the Communication Assistance to Law Enforcement Act (CALA), the implementation of state-of-the-art personal security features, and the explosion of telecommunication options (caller ID, call waiting, call conferencing, etc.) spotlighted the deficiencies of the legacy systems.

The Digital Collection Program provides the FBI with the means to collect evidence
and intelligence through the acquisition, deployment, and support of communications interception techniques and systems which facilitate and support national security, domestic counterterrorism, and criminal investigative efforts. Systems provided through this program intercept multi-source digital (and analog) communications information for intelligence gathering for foreign counterintelligence activities and investigative purposes for providing evidence of criminal activity for trial. It should be noted that those systems used for criminal investigations possess a requirement to minimize intercepted voice sessions (i.e., record only when the call is being actively monitored). Electronic information collected includes pen register (incoming and outgoing dialed digits, caller identification, date/time of communication, and other signal related information), analog and digital telephone calls, facsimile and modem transmissions, and microphone audio. High density drives and magneto-optical disks are utilized for temporary and permanent storage, respectively; no special, environmental storage facilities are needed. Digital Collection systems are used primarily by FBI Field offices and Resident Agencies in support of active foreign intelligence and criminal cases. Support is also provided to other federal, state, local and tribal agencies, as required.

The Digital Collection Program has evolved during its life cycle and has become more complex. Even so, digital collection systems are computer-based systems comprised primarily of commercial-off-the-shelf hardware and software with limited proprietary application software. Incorporated technological advances allow Case Agents to easily and effectively manage the recordings electronically, which dramatically increases the efficiency of trial preparations. While each Field Office or Resident Agency is self-sustaining in its ability to process intercepted information, this program permits interconnectivity of all FCI systems via a wide area network established to link Field offices' central monitoring plants for the purpose of digital collection information sharing it will use Trilogy's network backbone) and TRILOGY (the FBI's enterprise wide area network being deployed to link field offices). This connectivity enables the transfer of electronic or digital files of intercepts to a remote or distant field office for special language translation/transcription and sharing of information among FBI offices and other partnering agencies. Systems are also installed as fixed systems in locations that require long-term, permanent operations. In many instances, intercepted audio is shared via a secure, wide area network or downloaded from computer memory onto removable media and provided to language specialists in offices around the country, greatly increasing productivity of FBI translation and transcription efforts.

UNCLASSIFIED
<table>
<thead>
<tr>
<th>Project</th>
<th>Status</th>
<th>CRS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY08-032 FBI Digital Collection</td>
<td>Completed</td>
<td>CRS</td>
<td>Collects audio, microphone, and fax intercepts. A PIA is not required pursuant to the E-Government Act because the FBI's Digital Collection Systems are considered national security systems. However, the FBI conducts internal PIAs on all national security systems to ensure that privacy rights are adequately considered in system development. A PIA was conducted and approved 8/27/2001 for the digital collection systems. OTD performed an upgrade to the system in July of 2005. By EC dated 12/22/2005, OGC advised that a supplemental PIA was not required, and that OGC should be consulted for any subsequent upgrades.</td>
</tr>
<tr>
<td>FY08-033 Administrative Systems</td>
<td>Yes, unless it is a NSS</td>
<td>Required. Possibly covered by existing but may need update</td>
<td>Funding is requested to continue to expand and extend the set of IDW services and data provided. A PIA is not required pursuant to the E-Government Act because this is a national security system. However, the FBI conducts internal PIAs on all national security systems to ensure that privacy is adequately considered in system development. A series of PIAs have been conducted on IDW. Addition PIAs should be conducted as changes are made to the system.</td>
</tr>
<tr>
<td>FY08-034 IDW Base</td>
<td>Y</td>
<td>CRS</td>
<td>This investment funds the ongoing activities necessary to sustain the FBI HQ IT Centralized Cable Plant infrastructure. The cable plants are used to distribute the FBI's various networks to FBI facilities. As such, these projects do not involve the collection, maintenance or dissemination of identifiable data. Instead, they provide support for the networks that do transport data; as such no PIA/SORN required. Note - PIAs/SORNs are required for applications/service/content supported by the cable if these otherwise meet the PIA criteria. Note - E-300 mentions a cable management system (Visionael). If this system captures identifiable information a PIA may be required. Note - E-300 mentions an HQ IT trouble ticket management system- if only contains information about government employees, no E-government PIA required (internal system) but an FBI PIA is required.</td>
</tr>
<tr>
<td>FY08-035 Centralized Cable Plant</td>
<td>N (but see status/explanation)</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bureau Personnel Management System (BPMS)</td>
<td>4 PTAs: (1). BPMS-Address Locator Subsystem (ALS) (2) BPMS-Applicant Processing Subsystem (APS) (3) BPMS-Federal Parent Locator System (FPLS) (4) BPMS (composite PTA for remaining BPMS applications: Agency Parking Administration; BPMS Bulletin Board; Employee Self Query; Organization Inquiry; Travel Locator; Administrative Time Capture; Payroll; Agent Career Board; Agent Transfers; Batch Reporting; Counselor Matters; Critical Case Tracking; Drug Deterrence Program; Employee Benefits; Equal Employment Opportunity; General Reporting; Health Care Programs; Issued Personal Property; Job Postings Application for Special Agents: Personnel Ad Hoc Reporting; Office of Professional Responsibility; Leave Administration; Pay Administration; Performance Recognition; Personal Contact Update; Position Classification; SF-52 Requests; Skills; Staffing; Funded Staffing Levels; Training; Facility Security System; Random Personnel for Polygraph Testing; Five Year Reinvestigations; Security Clearance/Security Clearance Reporting; and Undercover Special Operations)</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Campus WAN</td>
<td>Campus WAN</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Chemical Network (ChemNet)</td>
<td>ChemNet</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CJIS WAN</td>
<td>CJIS WAN</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Combined DNA Index System (CODIS)</td>
<td>N/A (PIA previously conducted)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Commercial Payments Unit Invoice Management System (CPUIMS)</td>
<td>CPUIMS</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Computer Analysis Response Storage Area Network (CARTSAN)</td>
<td>CARTSAN</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CYBERTRANS II</td>
<td>CYBERTRANS II</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data Collection System 3000 (DCS-3000)</td>
<td>DCS-3000</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Digital Document Management System (DDMS)</td>
<td>DDMS</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Document Capture System</td>
<td>Document Capture System</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Financial Management System (FMS)</td>
<td>FMS</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Field Office Integrity Security System (FOISS)</td>
<td>FOISS</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Forensic Audio, Video, and Image Analysis (FAVIA) LAN</td>
<td>FAVIA LAN</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Innocent Images Case Management System (IICMS)</td>
<td>N/A (PIA previously conducted)</td>
<td></td>
</tr>
</tbody>
</table>
Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION DOCUMENTS

Section: 36

Federal Bureau of Investigation
Here are some of the pics from the sysadmin room for our TIII/T50 equipment. Both the Voicebox network and
network are administered from that room. Our DCS3000 systems, an FBI net computer, the transportable
system, all of our slave controllers and patch panels for our collection lines are contained in this one 9'x12' room.

On the 6' workstation we have the following Voicebox components (which are all minitowers):

Server

Monitors,

We also have the following DCS3000 equipment on the same rack

CPU, DCS3000 criminal CPU, DCS3000 FISA CPU, 4 port FBI net CPU, an HP Printer, 3 UPS, an Edgeport

Then in the double rack system on the left side as you enter the room we have all our rack mounted slave controller
equipment, patch panels, latchbox panels, and other JSI legacy equipment.

I'm of the opinion that if we can wait on the equipment upgrade until we move into our new office it would save
everyone a lot of work and headaches. If we have to go with the equipment upgrade right now we may want to coordinate
the DCS3000 equipment upgrade so all we have to worry about finding a monitoring station for will be the FBI net cpu, the
printer, all the non-rack mountable UPS, the modems and routers, the monitors (unless we can run
everything but the FBI net cpu thru one 8 port then we'd only have two monitors) and the binders.

Let us know what you think. I think the DCS3000 folks were considering waiting on our upgrade to rackmount until we
move into our new office. Seems like we'd be doing the same work a second time inside of two years' when we move to
our new office.

Thanks John!
FW: Remote VoiceBox Networking

I've been asked to look into the possibility of extending our Charlotte-based VBII network to an outlying offsite, about 5 miles away. I spoke with [name] while he was here this week updating our VBIII system and he said that remote workstations could be networked into the rack system at Charlotte. He also mentioned that Chicago was participating in a pilot project that accomplishes a similar objective.

We are only two TTAs here with no plant support so I am trying to get a handle on the complexity of this type of project. In general terms, what are the costs in time, money, personnel? How much coordination is involved with vendors, ERF, security division, physical facilities unit, local ETs, local security and physical plant personnel? What kinds of equipment would be necessary and who would spec the job and provide the gear and installation? From Chicago I understand that we would require, at minimum, the remote clients (provided by ERF via JST), minimum 128K circuit between main site and remote (is this one circuit per client?), circuit for the DCS3000 (bandwidth required?), two routers (main site & client site provided by ERF), and a PIX Firewall (also provided by ERF). These are some of the questions I will need to find answers for before I give a response to our management regarding this proposal.

I appreciate any help you can provide. Thanks!
UNCLASSIFIED
NON-RECORD

I just got back in the office so I apologize for not getting back with you sooner. As I would love to inform you of our testing of the remote VB clients, I unfortunately will be unable to reply in an expeditious manner at this time. I ask that you contact (ERF) regarding this as he would have better information in most of the areas of question. I can then provide follow-up answers or possibly fill-in the blanks. In generic terms, here is what is involved:

Remote Clients - Provided by ERF through vendor

Minimum 128K circuit between main site and remote (We have a separate T1 for one of our remote sites and the other we are using the T1 for the DCS3000) - Site would have to pickup cost

(2) Routers - (Main site & Client Site) - Provided by ERF

PIX Firewall - Provided by ERF

Time frame to setup once circuit is up is no more than two days (as long as there are no major issues)

I've been asked to look into the possibility of extending our Charlotte-based VBIII network to an outlying offsite, about 5 miles away. I spoke with (ERF) while he was here this week updating our VBIII system and he said that remote workstations could be networked into the rack system at Charlotte. He also mentioned that Chicago was participating in a pilot project that accomplishes a similar objective.

We are only two TTAs here with no plant support. I am trying to get a handle on the complexity of this type of project. I'd like to ask you, in general terms, what are the costs in time, money, personnel? How much coordination is involved with vendors, ERF, security division, physical facilities unit, local ETs, local security and physical plant personnel? What kinds of equipment would be necessary and who would spec the job and provide the gear and installation? These are some of the questions I will need to find answers for before I give a response to our management regarding this proposal.

I appreciate any help you can provide. Thanks!

FBI Charlotte Division
(704) 66
d7C

UNCLASSIFIED
Yahoo! We'll watch for it. Thanks again,

---Original Message-----
From: OTD (FBI)
Sent: Tuesday, September 19, 2006 5:39 AM
To: LA (FBI)
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

Offline Analysis Workstation is being shipped today with inkjet printer. OAW should be returned to ERF at some point but please do not return the printer.

No PointSec installed, it crashed the first system we tried to put it on.

Windows and VoiceBox user accounts are the same and are as follows:
User: 
Password: 

Please create additional accounts for your user to use.

Desk - 703
Cell - 202

---Original Message-----
From: OTD (FBI)
Sent: Tuesday, September 12, 2006 3:10 PM
To: LA (FBI)
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

OK, thanky

---Original Message-----
From: OTD (FBI)
Sent: Tuesday, September 12, 2006 11:49 AM
To: LA (FBI)
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD
Speaking with [redacted] this morning I believe the [redacted] issue was resolved.

I did receive a VoiceBox Review WS recently but we have not been able to get Pointsec loaded on it. We are working to acquire a more up to date version of Pointsec to see if it will make a difference. Also we are short staffed at the moment and have been given numerous other priorities as each day unfolds. I am in NY this week and hope to be able to address the issue with Pointsec next week when I return.

--- Original Message ---

From: (LA) (FBI)  
Sent: Monday, September 11, 2006 7:28 PM  
To:  
Cc: (OTD) (FBI)  
Subject: Voice Box Question  

UNCLASSIFIED  
NON-RECORD  

We currently have [redacted]. For some reason the [redacted] CDC input keeps going down in Voice Box. Yet, on the DCS3000 network the connection to [redacted] is fine. Why would the connection be dropping on Voice Box? Should we call the help line? Or is this a problem with which you are familiar?

PS- Have you received the portable Voice Box review stations yet? The case agent here in LA keeps bugging us about this.
Offline Analysis Workstation is being shipped today with inkjet printer. OAW should be returned to ERF at some point but please do not return the printer.

No PointSec installed, it crashed the first system we tried to put it on.

Windows and VoiceBox user accounts are the same and are as follows:
User: [redacted]
Password: [redacted]

Please create additional accounts for your user to use.

Desk - 703
Cell - 202

-----Original Message-----
From: [redacted]
Sent: Tuesday, September 12, 2006 3:10 PM
To: [redacted]
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

OK, thanks

-----Original Message-----
From: [redacted]
Sent: Tuesday, September 12, 2006 11:49 AM
To: [redacted]
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

Speaking with [redacted] this morning I believe the [redacted] issue was resolved.

I did receive a VoiceBox Review WS recently but we have not been able to get Pointsec loaded on it. We are working to acquire a more up to date version of Pointsec to see if will make a difference. Also we are short staffed at the moment and have been given numerous other priorities as each day unfolds. I am in NY this week and hope to be able to address the issue with Pointsec next week when I return.

Desk - 703
Cell - 202
We currently have [a] [Tll]. For some reason the [CDC] input keeps going down in Voice Box. Yet, on the [DCS3000] network the connection is fine. Why would the connection be dropping on Voice Box? Should we call the help line? Or is this a problem with which you are familiar?

PS- Have you received the portable Voice Box review stations yet? The case agent here in LA keeps bugging us about this.
From: LA (FBI)
Sent: Tuesday, September 12, 2006 3:10 PM
To: (OTD) (FBI)
Subject: RE: Voice Box Question

OK, thanks.

-----Original Message-----
From: OTD (FBI)
Sent: Tuesday, September 12, 2006 11:49 AM
To: LA (FBI)
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

Speaking with this morning I believe the issue was resolved.

I did receive a VoiceBox Review WS recently but we have not been able to get Pointsec loaded on it. We are working to acquire a more up to date version of Pointsec to see if will make a difference. Also we are short staffed at the moment and have been given numerous other priorities as each day unfolds. I am in NY this week and hope to be able to address the issue with Pointsec next week when I return.

Desk- 703
Cell - 202

-----Original Message-----
From: LA (FBI)
Sent: Monday, September 11, 2006 7:28 PM
To: OTD (FBI)
Cc: LA (FBI)
Subject: Voice Box Question

UNCLASSIFIED
NON-RECORD

We currently have a III. For some reason the CDC input keeps going down in Voice Box. Yet, on the DCS3000 network the connection to is fine. Why would the connection be dropping on Voice Box? Should we call the help line? Or is this a problem with which you are familiar?

PS: Have you received the portable Voice Box review stations yet? The case agent here in LA keeps bugging us about this.

UNCLASSIFIED
From: (OTD) (FBI)
Sent: Tuesday, September 12, 2006 2:49 PM
To: (OTD) (FBI)
Subject: RE: Voice Box Question

UNCLASSIFIED
NON-RECORD

Speaking with [__] this morning I believe the [__] issue was resolved.

I did receive a VoiceBox Review WS recently but we have not been able to get Pointsec loaded on it. We are working to acquire a more up to date version of Pointsec to see if will make a difference. Also we are short staffed at the moment and have been given numerous other priorities as each day unfolds. I am in NY this week and hope to be able to address the issue with Pointsec next week when I return.

Desk: 70
Cell: 202

---Original Message---
From: (OTD) (FBI)
Sent: Monday, September 11, 2006 7:28 PM
To: (OTD) (FBI)
Cc: (LA) (FBI)
Subject: Voice Box Question

UNCLASSIFIED
NON-RECORD

[__]

We currently have a [__] problem. For some reason the [__] CDC input keeps going down in Voice Box. Yet, on the DCS3000 network the connection to [__] is fine. Why would the connection be dropping on Voice Box? Should we call the help line? Or is this a problem with which you are familiar?

PS- Have you received the portable Voice Box review stations yet? The case agent here in LA keeps bugging us about this.

UNCLASSIFIED

UNCLASSIFIED
We currently have a problem with the Voice Box. For some reason the CDC input keeps going down in Voice Box. Yet, on the DCS3000 network the connection to a line. Why would the connection be dropping on Voice Box? Should we call the help line? Or is this a problem with which you are familiar?

PS- Have you received the portable Voice Box review stations yet? The case agent here in LA keeps bugging us about this.
All,

This is to recap the discussion/test that we did on the VB this morning. First, the problem statement:

Incoming calls where both target and associate are within the same switch may only populate the CALEA Temination Attempt message "Calling Party" identification field with the MIN (Mobile Identification Number). The MIN is not guaranteed to be the calling party's phone number (it is a valid 10 digit number) and is being populated in the VB as the CALLING PARTY'S phone number.

Through analysis, it is seen that the subsequent "Network Signal" message has within it a "CALLING PARTY" field with the caller id of the calling party. This has come up in several cases and specifically I have had several conversations with the Chicago FO about the affect this has on their Title III's and requests for potential pans off this FALSE information.

The DCS 3000 currently looks for the "Calling Party" id in the Calling DN field only. This problem should be addressed with JSI for the VB and for the

SENSITIVE BUT UNCLASSIFIED
Some additional equipment from JSI was already shipped and received at Chicago for this install, it needs to be added to the property database for your site.

We will be sending out a couple of routers and a switch to Chicago this week. Also an additional PIX may ship early next week.

I will temporarily send our multi CD player and patch panel next week for testing purposes.

Let me know on Monday when the T1 line is confirmed. I plan to travel out on Tuesday if all goes well.
I received word today that the WRA has a T-1 available for a T-III that could be coming as soon as July. Chicago can supply workstations for the test and leave a couple out there for the T-III. How long does the testing take? We also have a T-1 out to RRA if you want to do some testing out there.

--- Original Message ---
From: (CG) (FBI)  
Sent: Tuesday, May 30, 2006 9:08 AM  
To: (CG) (FBI)  
Cc: (CG) (FBI)  
Subject: UNCLASSIFIED NON-RECORD

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is ______ with ______ as a second possible location.

Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired. I believe that you informed me that Chicago does not have a circuit to the ______ at this time but may still have one for the ______. I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1.

You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test? I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk- 703  
Cell - 202

--- Original Message ---
From: (OTD) (FBI)  
Sent: Tuesday, June 06, 2006 12:38 PM  
To: (CG) (CON)  
Cc: (OTD) (FBI)  
Subject: UNCLASSIFIED NON-RECORD
The T-1 will be ready on Monday.

How well is the T1 installation going for the...? This looks to be the largest unknown at the time the whole schedule will be dependent upon it being completed.

I also ordered 5 additional AWS workstations, 1 additional printer and 1 remote host machine that can be used at the sites. They should be arriving at the Chicago office before the July 10 date we are working with.

More scheduling information to follow.

Desk - 703
Cell - 202
Subject:

UNCLASSIFIED
NON-RECORD

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is [redacted] with [redacted] as a second possible location.

Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired.

I believe that you informed me that Chicago does not have a circuit to the [redacted] at this time but may still have one for the [redacted].

I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1.

You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test?

I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk - 703
Cell - 202
UNCLASSIFIED
NON-RECORD

All - Attached in the message below is the OIG's "final" list of documents they have not received concerning the DCS-3000, DCS-5000, and DCS-6000. Please review your records and forward to me any documents you find. I will forward them to the OIG.

Thanks.

-----Original Message-----
From: [Name] (OTD) (FBI)
Sent: Monday, July 03, 2006 3:26 PM
To: [Name] (OTD) (FBI)
Cc: [Name] (OTD) (FBI)
Subject: FW: OIG Audit of Information Technology Research, Plans, Studies and Evaluations

UNCLASSIFIED
NON-RECORD

Hello:
I just received an e-mail from the OIG regarding documents that were not received pertaining to Digital Collection. I know you are in the process of giving me additional documents. I am attaching the list of items, so that you could compare your list with the OIG. I will continue to collect the documents from the S: drive.

DIGITAL COLLECTION.pdf (936 k)

Thank you,

[Name]

UNCLASSIFIED
From: OTD (FBI)
Sent: Thursday, June 29, 2006 2:59 PM
To: BS (CON) (FBI)
Subject: Boston upgrade notes

UNCLASSIFIED
NON-RECORD

Please ship toolbox back to ERF to TICTU.

A [ ] and cables should be shipped from ERF to [ ] to connect the both DCS3000 machine and the one way push LO side machine to the keyboard/monitor device.

JSI has an open ticket for the bad AWS 13 machine, they should be sending a replacement power supply.

One of the [ ] is bad, JSI will need to be called and start a trouble ticket on it to be repaired, most likely it will need to be sent to JSI in Sterling, VA. 866 [ ].

I emailed instructions on how to setup VirusScan on the AWS machines, I was only able to do AWS1, the rest still need to be done.

I told [ ] that I called JSI and I am having them replace the screens for the AWS machines, you should be getting 14 new flat panel screens for the 14 AWS machines, they may come with built in speakers but don’t use them, I here that the speaker portion works poorly. Try not to lose the new screens on other machines.

I also am having JSI send a replacement for CDR2, the replacement will also record to DVD. Once the new system is in then the old CDR2 should be excessed, no more support will be available for it from ERF.

[ ] got the new wiring in but the VB UPSs were tripping the breaker, he said that he would correct the problem with the breakers when he returns from vacation. Extension cords for the time being!

I spoke with [ ] at JSI about trying to see if the Providence upgrade to 3.6 could be done soon, please follow up with JSI to see if it will be possible. 866 [ ].

I will be out next week until Thursday.

Your [ ] program will need to be loaded on the new VBSVR machine to remote control Providence.

The old VoiceBox servers may be excessed or redistributed. ERF will no longer support any of these devices. You may need the front covers for the Providence system.

Desk - 703
Cell - 202
The T-1 was ordered but I don't have a due date yet. I'll keep you up to date as the info comes in.

--- Original Message ---
From: (OTD) (FBI)
Sent: Tuesday, June 20, 2006 4:48 AM
To: CG) (FBI)
Subject: RE: Chicago remote VB

UNCLASSIFIED
NON-RECORD

How well is the T1 installation going for the (OTD) (FBI) This looks to be the largest unknown at the time the whole schedule will be dependent upon it to be completed.

I also ordered 5 additional AWS workstations, 1 additional printer and 1 remote host machine that can be used at the sites. They should be arriving at the Chicago office before the July 10 date we are working with.

More scheduling information to follow.

--- Original Message ---
From: (OTD) (FBI)
Sent: Tuesday, June 06, 2006 12:38 PM
To: OTD) (FBI); CG) (FBI)
Subject: RE:

UNCLASSIFIED
NON-RECORD

I received word today that the WRA has a T-1 available for a T-III that could be coming as soon as July. Chicago can supply workstations for the test and leave a couple out there for the T-III. How long does the testing take? We also have a T-1 out to RRA if you want to do some testing out there.

SECRET
Subject:

UNCLASSIFIED
NON-RECORD

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is [BLANK] with [BLANK] as a second possible location.

Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired.

I believe that you informed me that Chicago does not have a circuit to the [BLANK] at this time but may still have one for the [BLANK].

I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1.

You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test?

I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk - 703
Cell - 202

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED
How well is the T1 installation going for the T-1? This looks to be the largest unknown at the time the whole schedule will be dependent upon it being completed.

I also ordered 5 additional AWS workstations, 1 additional printer and 1 remote host machine that can be used at the sites. They should be arriving at the Chicago office before the July 10 date we are working with.

More scheduling information to follow.

--- Original Message ---

I received word today that the WRA has a T-1 available for a T-III that could be coming as soon as July. Chicago can supply workstations for the test and leave a couple out there for the T-III. How long does the testing take? We also have a T-1 out to RRA if you want to do some testing out there.

--- Original Message ---

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is [ ] with [ ] as a second possible location.
Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired.

I believe that you informed me that Chicago does not have a circuit to the [redacted] at this time but may still have one for the [redacted].

I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1.

You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test? I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk - 703
Cell - 202
Gents,

I want to provide you with a "heads-up" as to a presentation I will most likely be putting together this Fall. It is high level and will be needing some assistance to complete. Thanks.

Hi [Name],

Here is the ITAB template. When [Name] gets in tomorrow, I will see what Powerpoint presentations she has on the DCS-3000, DCS-5000 & DCS-6000 and try to incorporate as much as I can.

Thanks

Hi [Name],

Thanks for your inquiry.

Yes, the briefing is high-level. The ITAB members are all Assistant Directors - from all FBIHQ divisions.

Attached is the template that the CIO established as the standard for all ITAB briefings. Use this as your guide and it is specific about the kind of information requested.
If you need any further guidance/assistance, please contact me.

Thanks again,

Blackberry: 202
ITAB
late-May06.ppt (1)

Original Message:
From: OTD (CON)
Sent: Friday, June 16, 2006 11:20 AM
To: OCIO (CON)
Subject: FW: ITAB Briefing Schedule
Importance: High

UNCLASSIFIED
NON-RECORD

Hello,

I have been tasked with putting together this presentation for TICTU/DCS. In your initial email, you mentioned that you would be sending out a template for these presentations. If you have one, would you please forward it along to me? I know if you do have a template—that will be a good starting point for me to start working from.

I also wanted me to ask the type of information you are looking for us to present? I see from your initial email that you want the presentation length to be around 20 minutes so it looks like you want to keep things at a high level.

Please advise.

Thank you.

703

Here is the information wanted me to pass on to you.

OTD/ESTS/TICTU
703

Original Message:
From: OTD (CON)
Sent: Thursday, May 04, 2006 4:59 PM
To: OTD (CON)
Cc: FBI
Subject: FW: ITAB Briefing Schedule
Importance: High
I received word today that the WRA has a T-1 available for a T-III that could be coming as soon as July. Chicago can supply workstations for the test and leave a couple out there for the T-III. How long does the testing take? We also have a T-1 out to RRA if you want to do some testing out there.

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is _______ with _______ as a second possible location.

Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired.

I believe that you informed me that Chicago does not have a circuit to the _______ at this time but may still have one for the _______.

I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1.

You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test? I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk - 70  
Cell - 202
From: IFCYRM (FBI)
Sent: Tuesday, May 30, 2006 10:08 AM
To: (OTD) (FBI)
Cc: (OTD) (FBI)

Here is what I have so far for Chicago to be a test site for remote VoiceBox, we will need to move quickly for completion by the date we discussed earlier.

Discussed installation date of VoiceBox equipment and initial test. Begin on Monday July 10th.

Desired location is with as a second possible location.

Circuits would need to be operational before this time. Chicago may work with our DCS3000 lab in acquiring circuits if desired.

I believe that you informed me that Chicago does not have a circuit to the at this time but may still have one for the

I was also informed that Chicago would pay for the circuit to each location. The desired circuit for each would be a full T1. You had mentioned that the circuits would be temporary and only for the operation of the specified case that the office will work. With the remote setup the circuit would need to remain up as long as case review was needed at the RA or the case could be processed at the Chicago FO once monitoring was over and a circuit discontinued.

Will Chicago be able to supply the AWS workstations from the FO to the remote sites for this test? I believe we had mentioned 4 AWSs for the remote site. ERF would also add a remote site repository machine with CDR capability and a printer.

Looking forward to your response.

Desk - 703
Cell - 202

UNCLASSIFIED
This can be done if needed. You will need to submit one RMS for a system and one also for the DCS3000 group if they do not currently have that ability.

Hey

Thanks for all the equipment.

Plantation is going up on their wire this week and everything is working perfectly.

Now the big question, West Palm Beach wants to go up on a wire around June. Can Miami get another portable VoiceBox system? I told them no, but SSA wanted me to ask you formally.

Thanks.

P's submit a request to ERF for a port. VB for this case.
I am the case agent re: We have drafted a TIII Affidavit and expect to go up in June 06'. I spoke to re: a voicebox for the PBCRA so that we can monitor at West Palm Beach. He said we needed to send you a formal request. I understand that we may have to borrow a voicebox from Quantico. Anything you can do will be appreciated. Thanks!

561 cell
561 office

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED
FYI!

This bulletin was brought to our attention yesterday. We didn't know if you guys had seen this back in the lab, so we thought we would send it your way. This bulletin refers to counterfeit parts within the routers.

We have the same 2600 series installed for our DCS3000 unit. We have not verified the part numbers yet, because it will require us to remove the router from the rack and possibly power it down to look inside. Do you have any guidance on checking inside the router without taking it down?
Hi all,

There has been a slight change to the IP address plan for the Chicago move. We have temporarily allocated a new block of IPs to the old building and a new block to the new building. Here is the list of events that need to happen:

1. Add new block of IPs to old building.
   - This has already been done with the main router set for 7th RA scheme. Use this as the gw.
2. a. Change the IPs for the portable VB at the old building to use the 7th RA scheme.
   b. Change the one way push boxes at the old building to use the 7th RA scheme.
3. Install new circuit to new building with ip addresses of 8th RA scheme.
   - The main router will be installed with ip addresses of 8th RA scheme. Use this as the gw.
4. a. VB at new building should be setup to use IPs for 8th RA scheme.
   b. Change one way push boxes at new building should be setup for 8th RA scheme.
5. When Chicago is ready, move DCS-3000 machines and main FO IPs to the new building. No ip changes will need to be made to these machines.
6. a. Change VB IPs at new building to main FO IP scheme.
   b. Change one way push IPs to main FO IP scheme.
   *** Note: The above step is optional, but recommended ***
7. When service at old building no longer needed, shut down circuit.

Going with this plan will make the transition much more simple. The drawbacks are having to change the VB addresses after the systems are up and running, or, if we skip step 6, then the waste of a block of IPs.

If anyone has any questions about this, please give me a call.

thanks!

703

UNCLASSIFIED
After adding new switch inputs to our Service Provider in the DCS6000 and trying to ping them the only response we got was from the already existing StLouis input. I used the IP addresses taken from the DCS3000 website; they were as follows:

(S) Houston
(S) Phoenix
(S) Denver

All ping replies timed out except St Louis. Do we need to add anything to our DCS3000 PIX Firewall routing table to be able to get out to these sites? Do you have any idea what we might be doing wrong here?
We have one of our small DCS-6000 available for demo at the OTD Tech EXPO today until 3PM. We are down in the Flag Room here at HQ. Come down and bring others from your group to check us out.

Desk - 703
Cell - 202

-----Original Message-----
From: SecD (CON)
Sent: Wednesday, April 26, 2006 8:51 AM
To: SecD (CON)
Cc: SecD (CON)
Subject: DCS-6000 Accreditation Diagram

All,

Attached is a network diagram I did based on the current documentation. Please take a look and let me know if it is accurate. I need to get the Tier EC done. Also, can you update the Registration forms for DCS-3000 and DCS-6000. I want to ensure the POC's in the EC are correct.

Regards, << File: DCS-6000 Accreditation Boundary Diagram.vsd >> << File: DCS-6000 Accreditation Boundary Diagram.doc >>

SecD/IAS/AU
(202)

-----Original Message-----
From: SecD (CON)
Sent: Thursday, April 27, 2006 7:09 AM
To: SecD (CON)
Subject: RE: DCS-6000 Accreditation Diagram
All,

Attached is a network diagram I did based on the current documentation. Please take a look and let me know if it is accurate. I need to get the Tier EC done. Also, can you update the Registration forms for DCS-3000 and DCS-6000. I want to ensure the POC's in the EC are correct.

Regards,

DCS-6000 Accreditation Diagram

DCS-6000 Accreditation Diagram

SECRET
Hello y'all - I'm seeking your advice to hopefully save a lot of work. I'm an ET in Dallas, just returned from Security training and has been designated the computer/network security person for our Division (ISSO?). He advised that HQ has mandated that he obtain all sorts of info from our systems/networks i.e: DCS 1000, DCS 3000, DCS 5000, DCS 6000 etc.

He wants an accounting for all of the systems we, as TTAs & DCSPs, maintain. He wants to have diagrams, schematics, charts etc on what we have and how everything is connected. He wants lists of all of the general users and all of the limited/admin users.

Is this duplicating what has already been done @ ERF w/ the security certification for each system? Or is there a new mandate to have this info on file w/ the specifics for each individual field office?

I also discussed restrictions regarding contractors and non employees working on, touching our systems. He even mentioned the phone company installers when they come to install/troubleshoot circuits etc. My understanding from this conversation is that they are not suppose to bring in computers, test equipment, etc that have memory etc. We are suppose to supply the computers/equipment for them to use.

I know that when JSI comes to install our new VoiceBox, the week after next, that they will have their own computers, flash drives etc. I know that when _______ was just here to upgrade our database they brought in laptops. SBC installers bring in test equipment & laptops _______ will have equipment to test the new DCS 3000 network connection in the new Frisco RA in the next couple of weeks.

How can we best handle this situation? Do I need to get a copies of the certification documents from ERF to give to _______ or should we just walk him through our system and have him make diagrams. Is there something in writing that I can read to better understand what I have to do when, SBC, JSI, etc come into our space?

Any advice, comments etc would be helpful.
From: (OTD) (FBI)  
Sent: Monday, April 24, 2006 11:57 AM  
To: (OTD)(CON)  
Subject: FW: DCS 6000 Meeting Kickoff meeting attendance sheet for 19 April 2006  

UNCLASSIFIED  
NON-RECORD  

Also I left me a message that someone in our meeting with them was expecting an updated system drawing. Can you call about this?

--- Original Message ---  
From: (SecD)(CON)  
Sent: Monday, April 24, 2006 11:51 AM  
To: (OTD) (FBI)  
Cc: (SecD) (FBI); (SecD) (CON)  
Subject: DCS 6000 Meeting Kickoff meeting attendance sheet for 19 April 2006  

UNCLASSIFIED  
NON-RECORD  

Please pass to  

DCS 6000 Meeting 19th April 2006  

<table>
<thead>
<tr>
<th>ISSM</th>
<th>SECD/IAS/AU</th>
<th>TICTU/OTD</th>
<th>TICTU/ISSO</th>
<th>SECD/IAS/CU</th>
<th>SECD/IAS/CU</th>
</tr>
</thead>
<tbody>
<tr>
<td>703</td>
<td>202</td>
<td>703</td>
<td>b6</td>
<td>b7c</td>
<td></td>
</tr>
</tbody>
</table>

DCS 3000 Meeting 19th April 2006  

<table>
<thead>
<tr>
<th>OTD</th>
<th>ISSM</th>
<th>SECD/IAS/AU</th>
<th>ISSO</th>
<th>SECD/IAS/CU</th>
<th>SECD/IAS/CU</th>
</tr>
</thead>
<tbody>
<tr>
<td>703</td>
<td>703</td>
<td>202</td>
<td>703</td>
<td>202</td>
<td>b7c</td>
</tr>
</tbody>
</table>
**DCS 6000 Meeting 19th April 2006**

<table>
<thead>
<tr>
<th>ISSM</th>
<th>703</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECD/IAS/AU</td>
<td>202</td>
</tr>
<tr>
<td>TICTU/OTD</td>
<td>703</td>
</tr>
<tr>
<td>TICTU/ISSO</td>
<td></td>
</tr>
<tr>
<td>SECD/IAS/CU</td>
<td>202</td>
</tr>
<tr>
<td>SECD/IAS/CU</td>
<td>202</td>
</tr>
</tbody>
</table>

**DCS 3000 Meeting 19th April 2006**

<table>
<thead>
<tr>
<th>OTD</th>
<th>703</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSM</td>
<td>703</td>
</tr>
<tr>
<td>SECD/IAS/AU</td>
<td>202</td>
</tr>
<tr>
<td>ISSO</td>
<td>703</td>
</tr>
<tr>
<td>SECD/IAS/CU</td>
<td>202</td>
</tr>
<tr>
<td>SECD/IAS/CU</td>
<td>202</td>
</tr>
</tbody>
</table>

---

**SecD/IAS/CU (Certification Unit)**

"Certification Lead Team #2"

Phone: (202)
Fax: (202)
From: [Redacted]
Sent: Monday, April 24, 2006 9:43 AM
To: [Redacted]
Cc: [Redacted]
Subject: RE: Security Issues w/ ERF/TTA Networks

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I have some guidance for the dcs6000. Thanks.

Since ERF is going to get these requests from everyone in the field, I suggest we wait for a unified reply from the ERF folks on the dcs1000, 3000, and 5000 platforms at which time we can show how Dallas has configured the interconnections, etc.

Any ideas?

-----Original Message-----
From: [Redacted]
Sent: Sunday, April 23, 2006 3:50 PM
To: [Redacted]
Cc: [Redacted]
Subject: Security Issues w/ ERF/TTA Networks

Hello y'all - I'm seeking your advice to hopefully save a lot of work. I am an ET in Dallas, just returned from Security training and has been designated the computer/network security person for our Division (ISSO?). He advised that HQ has mandated that he obtain all sorts of info from our systems/networks i.e: DCS 1000, DCS 3000, DCS 5000, DCS 6000 etc.

I want an accounting for all of the systems we, as TTAs & DCSPs, maintain. He wants to have diagrams, schematics, charts etc on what we have and how everything is connected. He wants lists of all of the general users and all of the limited/admin users.

Is this duplicating what has already been done @ ERF w/ the security certification for each system? Or is there a new mandate to have this info on file w/ the specifics for each individual field office?

He even discussed restrictions regarding contractors and non employees working on, touching our systems. He mentioned the phone company installers when they come to install/troubleshoot circuits etc. My understanding from this conversation is that they are not suppose to bring in computers, test equipment, etc that have memory etc. We are suppose to supply the computers/equipment for them to use.

I know that when JSI comes to install our new VoiceBox, the week after next, that they will have their own computers, flash drives etc. I know that when we was just here to upgrade our database they brought in laptops. Installers bring in test equipment & laptops will have equipment to test the new DCS 3000 network connection in the new Frisco RA in the next couple of weeks.

How can we best handle this situation? Do I need to get a copies of the certification documents from ERF to give to or should we just walk him through our system and have him make diagrams. Is there something in writing that I can read to better understand what I have to do when JSI, etc come into our space?

Any advice, comments etc would be helpful.
SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Given that JSI is coming here next week and since they made the systems (and we have absolutely no test equipment or knowledge of what the system settings should be) there is no rational alternative to them bringing their own stuff with them and to have complete access to the system. They of course will be escorted by CMP during their visit.

Thanks for supplying the dcs6000 ssp overview. As Sys Admin or as CMP mgr to get the list of Priv. users. I don't see the need for inventing any of this, if wants other diagrams, he should be present at the end of the JSI visit when we go over all the system changes, links, etc. I would suggest the time for that is at the end of the JSI install when we are repopulating the user lists. Any ideas?

---Original Message---

From: (OTD) (FBI)
Sent: Monday, April 24, 2006 9:40 AM
To: 7C
Cc: (DL)(FBI); (DL)(FBI); (DL)(FBI); (DL)(FBI); (DL)(FBI)
Subject: RE: Security Issues w/ ERF/TTA Networks

SS&RET

From: (OTD) (FBI)
Sent: Monday, April 24, 2006 9:40 AM
To: 7C
Cc: (DL)(FBI); (DL)(FBI); (DL)(FBI)
Subject: RE: Security Issues w/ ERF/TTA Networks

---Original Message---

From: (OTD) (FBI)
Sent: Monday, April 24, 2006 7:25 AM
To: 7C
Cc: (DL)(FBI); (DL)(FBI); (DL)(FBI); (DL)(FBI); (DL)(FBI); (DL)(FBI)
Subject: RE: Security Issues w/ ERF/TTA Networks

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

wants an accounting for all of the systems we, as TTAs & DCSPs, maintain. He wants to have diagrams, schematics, charts etc on what we have and how everything is connected. He wants lists of all of the general users and all of the limited/admin users.

Attached is the current SSP for the DCS6000 which should take care of the system diagrams and connections with much other information. The DCS6000 was accredited 3 years ago and is in the re-accreditation phase now, once this is completed we should have a new set of documents available in the summer or fall should have a list of all of the privilege users and general users as well as the signed user forms from all of these users.

also discussed restrictions regarding contractors and non employees working on, touching our systems. He even mentioned the phone company installers when they come to install/troubleshoot circuits etc. My understanding from this conversation is that they are not supposed to bring in computers, test equipment, etc that have memory etc. We are suppose to supply the computers/equipment for them to use.

The contractor equipment issue is technically correct but has been loosely enforced in the past. There is an EC that has been uploaded for the JSI foreign nationals to have access to the DCS6000 systems for installation and support and the SSP states that JSI personnel will need access to the system for support but must be escorted.

<< File: DCS6000_SSP_012506.doc >>

Overall the Bureau is working on trying to get all of its systems to be security accredited. But with the effort so far there are flaws. The documents that govern this process assumes that one standard fits all issues and also most personnel that are pulled into this effort and working towards the goals of compliance are learning as they go including the ones at the top.

The DCS6000 system is classified at Sensitive But Unclassified (SBU).

All need to check with the Chief Security Officer for your division to find out if JSI can bring there devices and laptop that they need in and out for the installs before they come so JSI can be advised if they cannot.
Hello y'all - I'm seeking your advice to hopefully save a lot of work. An ET in Dallas, just returned from Security training and has been designated the computer/network security person for our Division (ISSO?). He advised that HQ has mandated that he obtain all sorts of info from our systems/networks i.e: DCS 1000, DCS 3000, DCS 5000, DCS 6000 etc.

He wants an accounting for all of the systems we, as TTAs & DCSPs, maintain. He wants to have diagrams, schematics, charts etc on what we have and how everything is connected. He wants lists of all of the general users and all of the limited/admin users.

Is this duplicating what has already been done @ ERF w/ the security certification for each system? Or is there a new mandate to have this info on file w/ the specifics for each individual field office?

Also discussed restrictions regarding contractors and non employees working on, touching our systems. He even mentioned the phone company installers when they come to install/troubleshoot circuits etc. My understanding from this conversation is that they are not suppose to bring in computers, test equipment, etc that have memory etc. We are suppose to supply the computers/equipment for them to use.

I know that when comes to install our new VoiceBox, the week after next, that they will have their own computers, flash drives etc. I know that when was just here to upgrade our database they brought in laptops. Installers bring in test equipment & laptops. will have equipment to test the new DCS 3000 network connection in the new Frisco RA in the next couple of weeks.

How can we best handle this situation? Do I need to get a copies of the certification documents from ERF to give to or should we just walk him through our system and have him make diagrams. Is there something in writing that I can read to better understand what I have to do when etc come into our space?

Any advice, comments etc would be helpful.

---Original Message---

From: DL(FBI) Sent: 4:50 PM To: OTD (FBI) Cc: OTD (FBI) OTD (FBI) OTD (FBI) OTD

Subject: Security Issues w/ ERF/TTA Networks

SENSITIVE BUT UNCLASSIFIED

NON-RECORD

(49)

SECRET ×
Hello y'all - I'm seeking your advice to hopefully save a lot of work. A ET in Dallas, just returned from Security training and has been designated the computer/network security person for our Division (ISSO?). He advised that HQ has mandated that he obtain all sorts of info from our systems/networks i.e: DCS 1000, DCS 3000, DCS 5000, DCS 6000 etc.

He wants an accounting for all of the systems we, as TTAs & DCSPs, maintain. He wants to have diagrams, schematics, charts etc on what we have and how everything is connected. He wants lists of all of the general users and all of the limited/admin users.

Is this duplicating what has already been done @ ERF w/ the security certification for each system? Or is there a new mandate to have this info on file w/ the specifics for each individual field office?

Also discussed restrictions regarding contractors and non employees working on, touching our systems. He even mentioned the phone company installers when they come to install/troubleshoot circuits etc. My understanding from this conversation is that they are not suppose to bring in computers, test equipment, etc that have memory etc. We are suppose to supply the computers/equipment for them to use.

I know that when comes to install our new VoiceBox, the week after next, that they will have their own computers, flash drives etc. I know that when was just here to upgrade our database they brought in laptops. Installers bring in test equipment & laptops will have equipment to test the new DCS 3000 network connection in the new Frisco RA in the next couple of weeks.

How can we best handle this situation? Do I need to get a copies of the certification documents from ERF to give to or should we just walk him through our system and have him make diagrams. Is there something in writing that I can read to better understand what I have to do when, etc come into our space?

Any advice, comments etc would be helpful.
I submitted the RMS today (RMS Request Number: 0110431).

I spoke with the DCS3000 guys about getting the pen data to Chelsea and they can do it. Instead of the way we discussed with just piping over from our side of the PIX they have a task force office solution that they developed for situations like this which will add an additional DCS machine in the main office that will act as a buffer for the task force pen data and prevent any possibility of snooping for other data. We will need to get a RMS in for this equipment to the DCS3000 team as soon as possible.


As requested, here's a recap of what we discussed regarding upgrading the New York VoiceBox system to version 3.6. As we all know, there is never an ideal time that will not cause any impact.
From the standpoint of the impact on Title Ills, New York is presently running approximately [number] collections, of which [number] are consensuals that run continuously. It would be unusual for us to have fewer title IIIs that we currently have, and it is expected that all collections will increase due to an upcoming inspection scheduled for the fall. During the last inspection we had [number] active title IIIs, and a large number under review for trial.

To remove some of the pressure we have had in the past during upgrades, if we upgrade our [site] first, we can move [number] collections to that site. It would allow our personnel to gain experience with the new version while the CMP site is upgraded. We also now have some VoiceBox equipment at our RAs that might be used if needed.

I have spoken with one of our ETs, and if it is ok with ERF to do so, we can route the VBIIF pen data over to [site] using some spare bandwidth the ETs could provide on an existing link to Chelsea.

We have already sent [number] individuals through the version 3.6 training at JSI in Sterling, VA, so that should help during the switch to the new version.

Several cases are under review for trial, so we may need to export that data so the Agents have access to it if there is any long delay in completing the upgrade.

JSI expressed that he is comfortable with upgrading us. Cleveland had a very large database that provided a basis for how long the New York upgrade may take.

BAE - New York, is aware of the above and will be working on the [site] to ensure it is ready for the 3.6 upgrade (Service Pack installed, etc).

I will be speaking with the Case Agents to let them know of the possibility of the upgrade and to see if there is anything else to consider from their standpoint.
From:  
Sent:  Friday, March 31, 2006 8:10 AM  
To:  
Subject:  RE: New York VBIII Upgrade to 3.6

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I spoke with the DCS3000 guys about getting the pen data to Chelsea and they can do it. Instead of the way we discussed with just piping over from our side of the PIX they have a task force office solution that they developed for situations like this which will add an additional DCS machine in the main office that will act as a buffer for the task force pen data and prevent any possibility of snooping for other data. We will need to get a RMS in for this equipment to the DCS3000 team as soon as possible.

Desk - 703  
Cell - 202

-----Original Message-----
From:  
Sent:  Friday, March 31, 2006 3:19 AM  
To:  
Cc:  
Subject:  New York VBIII Upgrade to 3.6
Importance:  High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Reference our conversation Wednesday, 3/29/06, and my conversation with at JSI, Monday, 3/27/06, regarding upgrading the New York Voicebox system to version 3.6 in the near future.

As requested, here's a recap of what we discussed regarding upgrading the New York VoiceBox system to version 3.6. As we all know, there is never an ideal time that will not cause any impact.

From the standpoint of the impact on Title Ills, New York is presently running approximately collections, of which are consensuals that run continuously. It would be unusual for us to have fewer Tills that we currently have, and it is expected that all collections will increase due to an upcoming inspection scheduled for the Fall. During the last inspection we had active Title Ills, and a large number under review for trial.

To remove some of the pressure we have had in the past during upgrades, if we upgrade our site first, we can move collections to that site. It would allow our personnel to gain experience with the new version while the CMP site is upgraded. We also now have some VoiceBox equipment at our RAs that might be used if needed.

I have spoken with one of our ETs, and if it is ok with ERF to do so, we can route the VBIII pen data over to Chelsea using some spare bandwidth the ETs could provide on an existing link to

We have already sent individuals through the version 3.6 training at JSI in Sterling, VA, so that should help during the switch to the new version.

Several cases are under review for trial, so we may need to export that data so the Agents have access to it if there
is any long delay in completing the upgrade.

JSI expressed that he is comfortable with upgrading us. Cleveland had a very large database that provided a basis for how long the New York upgrade may take.

BAE - New York, is aware of the above and will be working on the site to insure it is ready for the 3.6 upgrade (Service Pack installed, etc).

I will be speaking with the Case Agents to let them know of the possibility of the upgrade and to see if there is anything else to consider from their standpoint.

CMF, New York
212 office
609 cell

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED
It appears that as of last week the CDC was being sent with the audio. There was no delay. We ran it with the CDC and CCC split all weekend and the Admin Agent monitored the timeliness of the CDC delivery and reported no delays. During this time she lost no audio, including during Call Waiting calls.

Everything appeared to work correctly until the audio was lost. So as not risk losing another pertinent call waiting call SA requested the CCC and CDC be received separately. I switched the Title III back to separated CCC and CDC at 20:05. (2014 VoiceBox time)

I was speaking to SA when I realized SA was letting her T-III expire tonight 03/27/06 @ 23:59. SA stops monitoring her two lines at midnight.

I decided to take this opportunity and reset the time on the VoiceBox system, since we are going up on another T-III 03/28/06 and possibly 3 more by the end of the week.
I am going to do the shutdown process (workstations, RWS1&2, CD-R 1&2, Site Manager). Then reset the time on the Server. Then power everything back up in reverse order (one at a time). Hopefully this will correct the time issue.

If there are any problems then you will receive another email from me. Otherwise No email = no problems.

Thank you

UNCLASSIFIED
This is tied primarily to future requests for money, 300 exhibits and requisition in FY07 and forward. However, the cost of each system should be looked at so we can determine our investment and support needs that are truly IT. We would like to know the cost of the part of each system that is IT (that allows our collection systems to connect to trilogy, operate remotely over an IT system, prepares data to be sent over/to an IT system).

I know this is a little vague but we need an estimate with some basis behind it.

Thanks.

TICTU personnel have asked that you specify what time period you are inquiring about, as well as defining what you consider IT to be. Are you asking about costs from the inception of projects that could date back years, or something else? Thanks.

Marcus Thomas has asked that we determine the cost of the IT portions of the OTD collection systems listed on the OCIO master list of systems, applications, databases, and networks. For the systems/projects listed below, please determine or estimate as best you can the cost of the hardware, software, and the development work for the interface to the Trilogy network or other FBI IT infrastructure. This will help us separate the funding of National Security Systems that are not truly IT from IT systems, databases, applications and networks. Please provide an estimate by Friday 3/24.
EDMS - IT Interface
DCS 6000 - IT Interface
DCS 3000 - IT Interface
DCSNet (CALEA transport)
CARTSAN - IT Interface
CART Family of Systems

Central Monitoring Plant Network
Central Monitoring Plant Systems Operations Center (CSOC)

Thanks,

ELSUR Management Technology Unit
Electronic Surveillance Technology Section, OTD
Phone: 703-
Cell: 202-
Fax: 703-

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED
The DCS6000 is a Title III telecommunications collection tool, it currently has no interface to Trilogy or other FBI-IT network. The DCS6000 does produce some reports that are sneaker-netted to TA and printed for ELSUR. The answer for now is zero dollars.

The DCS6000 does have a connection to the DCSNET for collection of CALEA data from intercepts. This network is paid for controlled wholly by the TICTU unit. This network also gives the DCS6000 the ability to perform some remote maintenance duties.

Looking to the near future the DCS6000 we do not see a connection directly to the Trilogy network as the DCS6000 is an unclassified network. We do see the need to develop a network that will allow us the bandwidth to process Title III telecommunications collections from remote offices while maintaining the core systems in central division offices for administrative purposes. It is unclear at this time if this would fall under a request for IT services or funded and maintained out of TICTU/Field Office operating expenses.

Pls see below.
This is tied primarily to future requests for money, 300 exhibits and requisition in FY07 and forward. However, the cost of each system should be looked at so we can determine our investment and support needs that are truly IT. We would like to know the cost of the part of each system that is IT (that allows our collection systems to connect to Trilogy, operate remotely over an IT system, prepares data to be sent over/to an IT system).

I know this is a little vague but we need an estimate with some basis behind it.

Thanks.
This is tied primarily to future requests for money, 300 exhibits and requisition in FY07 and forward. However, the cost of each system should be looked at so we can determine our investment and support needs that are truly IT. We would like to know the cost of the part of each system that is IT (that allows our collection systems to connect to trilogy, operate remotely over an IT system, prepares data to be sent over/to an IT system).

I know this is a little vague but we need an estimate with some basis behind it.

Thanks,
Marcus Thomas has asked that we determine the cost of the IT portions of the OTD collection systems listed on the OCIO master list of systems, applications, databases, and networks. For the systems/projects listed below, please determine or estimate as best you can the cost of the hardware, software, and the development work for the interface to the Trilogy network or other FBI IT infrastructure. This will help us separate the funding of National Security Systems that are not truly IT from IT systems, databases, applications and networks. Please provide an estimate by Friday 3/24.

EDMS - IT Interface
DCS 6000 - IT Interface
DCS 3000 - IT Interface
DCSNet (CALEA transport)
CARTSAN - IT Interface
CART Family of Systems
Central Monitoring Plant Network
Central Monitoring Plant Systems Operations Center (CSOC)
Marcus Thomas has asked that we determine the cost of the IT portions of the OTD collection systems listed on the OCIO master list of systems, applications, databases, and networks. For the systems/projects listed below, please determine or estimate as best you can the cost of the hardware, software, and the development work for the interface to the Trilogy network or other FBI IT infrastructure. This will help us separate the funding of National Security Systems that are not truly IT from IT systems, databases, applications and networks. Please provide an estimate by Friday 3/24.

**EDMS - IT Interface**
EDMS - IT Interface
EDMS 6000 - IT Interface
EDMS 3000 - IT Interface
DCSNet (CALEA transport)
DCS 6000 - IT Interface
CARTSAN - IT Interface
CART Family of Systems

Central Monitoring Plant Network
Central Monitoring Plant Systems Operations Center (CSOC)

Thanks,
UNCLASSIFIED
NON-RECORD

I believe below would be your unit’s call.
Please advise.

Thanks.

-----Original Message-----

From: (OTD) (FBI)
Sent: Tuesday, March 07, 2006 5:20 PM
To: [b7C] (OTD) (FBI)
Cc: (OTD) (FBI)
Subject: RE: Privileged User Role-Based Training

Even with the extension of time to complete the training associated with being a privileged user, we should probably identify which systems need to have the privileged user Rules of Behavior (ROB) created for. As I see it there are primarily three systems that are supported by the DCSP that each should have a ROB form. They are the System (DCS5000) the Voice Box System (DCS6000) and the DCS3000. My understanding is that each of these will be accredited at an enterprise level such that the system in Albany and the system in Portland both fall under a single ROB. But the three separate type of system each require their own ROB. So each system administrator will fill out three ROBs.

The form on the Security page only has a generic Rules of Behavior form that requires system name entry. To avoid confusion, I would recommend that TICTU identify how they want the system names to appear on the ROB. I believe that since each system is accredited separately that a unified “ELSUR Systems” ROB would not be in order.
Thanks, I was just inquiring just in case it was not thought of or became a stopping block as you moved forward.

In a recent discussion with the Office of the General Counsel, monitoring/collecting in different jurisdictions is not an issue. In *U.S. v. Denman*, 100 F. 3d 399 (5th Cir. 1996) the court stated "(w)e agree with the reasoning of the Second Circuit and now hold that interception includes both the location of a tapped telephone and the original listening post, and that judges in either jurisdiction have authority under Title III to issue wiretap orders." The original citing for this came from *U.S. v. Rodriguez* 968 F. 2d 130 (2d Cir. 1992). In this case, interception refers to where a communication is initially obtained regardless of where it is being heard. Also, to my knowledge the DEA has had no challenges to their hub (regional) collecting. I suggest you refer this matter to your CDC for additional guidance. The DCS-6000 team is still working on the technical end of making the remote workstation happen.

RMS# 105654 - Previously submitted requesting DCS6000 remote capability (Assigned to - Status is Working

SECRET × (74)
Per our discussion, here are some items of interest/or concern with regards to DCS6000 remote workstations. Also, I have talked with [REDACTED] and his is in agreement that Chicago would like to be a test site once this capability exists. We would be interested in an estimated time frame that this could happen and if there is anything that could be done to speed up the release of this technology.

Concerns/or Issues that may need to be addressed:

Legal - Monitoring/collection in different jurisdictions
Network - Minimum bandwidth, encryption
Security - Encryption, Accreditation

Possible requirements at a remote site:

Computer(s) (DCS6000/3000)
Router + (T1's (Network connection/data) and/or ISDN's)
Remote Server

- Chicago
ELSUR Technology Management Unit
Electronic Surveillance Technology Section, OTD
312 (Desk)
312 (Fax)
312 (Cell)
In a recent discussion with the Office of the General Counsel, monitoring/collection in different jurisdictions is not an issue. In *U.S. v. Penman*, 100 F.3d 399 (5th Cir. 1996) the court stated "(w)e agree with the reasoning of the Second Circuit and now hold that interception includes both the location of a tapped telephone and the original listening post, and that judges in either jurisdiction have authority under Title III to issue wiretap orders." The original citing for this came from *U.S. v. Rodriguez* 968 F.2d 130 (2d Cir. 1992). In this case, interception refers to where a communication is initially obtained regardless of where it is being heard. Also, to my knowledge the DEA has had no challenges to their hub (regional) collecting. I suggest you refer this matter to your CDC for additional guidance. The DCS-6000 team is still working on the technical end of making the remote workstation happen.

Per our discussion, here are some items of interest/or concern with regards to DCS6000 remote workstations. Also, I have talked with and he is in agreement that Chicago would like to be a test site once this capability exists. We would be interested in an estimated time frame that this could happen and if there is anything that could be done to speed up the release of this technology.

Concerns/or Issues that may need to be addressed:

Legal - Monitoring/collection in different jurisdictions
Network - Minimum bandwidth, encryption
Security - Encryption, Accreditation

Possible requirements at a remote site:
Computer(s) (DCS6000/3000)
Router + (T1's (Network connection/data) and/or ISDN's)
Remote Server

ELSUR Technology Management Unit
Electronic Surveillance Technology Section, OTD
312 Desk
312 Fax
312 Cell

UNCLASSIFIED

UNCLASSIFIED
Our vendor is in the process of rolling out an updated version of their application and we hope to start deploying this release in 2006. We will revisit the possibility of the inclusion in that release.

This is a follow-up to the meeting you had with TA on June 1, 2005. I was wondering if the contractors working on the J3094 voice box file made any progress with adding or using an existing field to the J3094 voice box file to indicate if a telephone number is...
This is a follow-up to the phone conversation that we had on June 2, 2005. I was wondering if you were able to agree on a meeting date. I will be on vacation on May 20, 2005 thru May 30, 2005. Could you tell me whether the CDNRS and J3094 data time are captures as real time or GMT? Will the contractor be able to add or use an existing field to the J3094 voice box file to indicate if a telephone number is

----Original Message----
From: (ITOD)(CON)
Sent: Friday, May 20, 2005 9:28 AM
To: (OTD) (FBI)
Subject: Pen Register

UNCLASSIFIED
NON-RECORD

From: (ITOD)(CON)
Sent: Friday, April 15, 2005 9:57 AM
To: (ITOD)(CON)
Subject: FW: Re current pen registers

UNCLASSIFIED
NON-RECORD

----Original Message----
From: 
Sent: Thursday, February 20, 2003 9:48 AM
To: 
Cc: 
Subject: Re: Re current pen registers

CM2210 (system no longer used) I am not sure if new format is used by another system.

ADNRS (system no longer used)

PCS (system no longer used)

CDNRS (system no longer used) But, upload format used by DCS3000

RDNRS (no longer used)

JSI - what format is this?

DISCOVERY - not being used

(80)
J3094 - format being used  
DCS - format being used  
DMW - format being used  

VOICE-ID - I did not know there was a format  
PINE - (system no longer used)  
NOKIA - I did not know there was a format  
DCSPC - is this similar to DCS?  

system being used; using DMW format  

ICD-14 - format being used  

Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.
This is a follow-up to the meeting you had with TA on June 1, 2005. I was wondering if the contractors working on the J3094 voice box file made any progress with adding or using an existing field to the J3094 voice box file to indicate if a telephone number is push-to-talk?

--- Original Message ---
From: (TOD)(CON)
Sent: Wednesday, May 18, 2005 10:41 AM
To: (OTD) (FBI)
Subject: RE: Pen Register

--- Original Message ---
From: [Redacted]
Sent: Friday, May 6, 2005 9:28 AM
To: (OTD) (FBI)
Subject: Pen Register

--- Original Message ---
From: [Redacted]
Sent: Friday, April 15, 2005 9:57 AM
To: [Redacted]
Subject: FW: Re current pen registers

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED
NON-RECORD
-----Original Message-----
From: 
Sent: Thursday, February 20, 2003 9:48 AM 
To:  
Cc:  
Subject: Re: Re current pen registers

CM2210 (system no longer used) I am not sure if new format is used by another system.

ADNRS (system no longer used)

PCS (system no longer used)

CDNRS (system no longer used) But, upload format used by DCS3000

RDNRS (no longer used)

JSI - what format is this?

DISCOVERY - not being used

J3094 - format being used

DCS - format being used

DMW - format being used

VOICE-ID - I did not know there was a format

PINE - (system no longer used)

NOKIA - I did not know there was a format

DCSPC - is this similar to DCS? system being used; using DMW format

ICD-14 - format being used

Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.

--- Original Message ---
From: 
Sent: Thursday, February 20, 2003 9:48 AM 
To:  
Cc:  
Subject: Re: Re current pen registers

CM2210 (system no longer used) I am not sure if new format is used by another system.

ADNRS (system no longer used)

PCS (system no longer used)

CDNRS (system no longer used) But, upload format used by DCS3000

RDNRS (no longer used)

JSI - what format is this?

DISCOVERY - not being used

J3094 - format being used

DCS - format being used

DMW - format being used

VOICE-ID - I did not know there was a format

PINE - (system no longer used)

NOKIA - I did not know there was a format

DCSPC - is this similar to DCS? system being used; using DMW format

ICD-14 - format being used

Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.
As per our telephone conversation about the two APC UPS malfunctioning (batteries swelling up), we were wondering if we could RMS the units or the batteries. The Unit serial number is SU1400RM2U. These units were installed by a contractor called AQC in 2002 when we moved to this building. They came and installed the racks that have the DCS 3000. Thanks.
UNCLASSIFIED

From: (OTD) (FBI)
Sent: Friday, January 13, 2006 2:39 PM
To: (OTD) (FBI)
Cc: (OTD) (FBI)
Subject: FW: DCS6000 Remote

--- Original Message ---

From: (OTD) (FBI)
Sent: Friday, January 13, 2006 12:10 PM
To: (OTD) (FBI)
Cc: (OTD) (FBI)
Subject: DCS6000 Remote

RMS# 105654 - Previously submitted requesting DCS6000 remote capability (Assigned to - Status is Working)

Per our discussion, here are some items of interest/or concern with regards to DCS6000 remote workstations. Also, I have talked with and his is in agreement that Chicago would like to be a test site once this capability exists. We would be interested in an estimated time frame that this could happen and if there is anything that could be done to speed up the release of this technology.

Concerns/or Issues that may need to be addressed:

Legal - Monitoring/collecting in different jurisdictions
Network - Minimum bandwidth, encryption
Security - Encryption, Accreditation

Possible requirements at a remote site:

Computer(s) (DCS6000/3000)
Router + (T1's (Network connection/data) and/or ISDN's)
Remote Server

Chicago
ELSUR Technology Management Unit
Electronic Surveillance Technology Section, OTD
312 (Desk)
312 (Fax)
312 (Cell)

--- Original Message ---
From: (CG) (CON)
Sent: Friday, January 13, 2006 12:10 PM
To: OTD (FBI)
Cc: CG (FBI)
Subject: RMS# 105654 - Previously submitted requesting DCS6000 remote capability (Assigned to - Status is Working

Per our discussion, here are some items of interest/or concern with regards to DCS6000 remote workstations. Also, I have talked with and his is in agreement that Chicago would like to be a test site once this capability exists. We would be interested in an estimated time frame that this could happen and if there is anything that could be done to speed up the release of this technology.

Concerns/or Issues that may need to be addressed:

Legal - Monitoring/collecting in different jurisdictions
Network - Minimum bandwidth, encryption
Security - Encryption, Accreditation

Possible requirements at a remote site:

Computer(s) (DCS6000/3000)
Router + (T1's (Network connection/data) and/or ISDN's)
Remote Server

Chicago

ELSUR Technology Management Unit
Electronic Surveillance Technology Section, OTD
312 Desk)
312 Fax)
312 Cell)
You are correct there is not a new date yet. [ERF] informed me that Yuma was originally scheduled for November 27th of 2006. [ERF] is leaving the Voice Box program for another department and he asked me to work with [JSI] with regards to moving the installation date up. I believe [JSI] will begin the 2006 installation schedule sometime in late February. I'm confident that [JSI] will let us know if they can move your date up. I have included him with this email.

Thanks,

---Original Message---

The VBIII upgrade equipment was delivered to the Yuma RA today. I expect that this delivery has no direct relationship to when the equipment will be installed, but that has not stopped [ERF] and everyone else from asking about it.

Unless you tell me differently, I am under the assumption that [ERF] is still finalizing their install schedule & they have not yet given a Yuma install date.

Please let me know if I am off track so I can keep the wolves at bay.

---Original Message---

Hi

Thanks for getting back so soon. The DCS lines will be Calea and should be fairly easy to move over to the VB. It's just a matter of getting the Telco to comply in a timely fashion. They will "Ring-Down" the POTS as indicated. We will have to let them know what POTS lines to call. I believe [ERF] are working on a solution for the
two "Orphan" lines. I suggested possibly getting ERF involved with installing the other equipment. We will ultimately make that decision. Thanks again and if I don't talk to you before then have a Merry Christmas.

Sincerely,

---Original Message---
From: (PX) (FBI)
Sent: Monday, December 19, 2005 10:57 AM
To: (PX) (CON)
Cc: (PX) (FBI) (PX) (FBL)
Subject: RE: Yuma's upcoming TIIIs

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

To further clarify your mission, two of the lines currently under collection on the DCS 3000 will be routed into the VB for audio collection. If any prep work is necessary for the VB transition of these two lines in particular, let me know, so we can plan for it.

Mathematically, that means we are bumping two current lines off the VB into the yet-to-be-determined alternate collection system.

Thanks for the assistance.

---Original Message---
From: (PX) (CON)
Sent: Monday, December 19, 2005 10:47 AM
To: (PX) (FBI)
Cc: (PX) (FBI)
Subject: RE: Yuma's upcoming TIIIs

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I have made plans to travel to AZ on January 4th and 5th to provide support for the Voice Box System. I will answer any software or hardware questions and stick around as long as necessary on Thursday. If it is determined that all current Trap/Trace targets which are found. There has been discussion of installing a rack mounted DNR with the others.

To be clear, my focus/support will be directed towards the Voice Box System not the alternate collection systems. During downtime I will be more than happy to provide any help I can with any tasks to complete the mission.

Regards,

Electronic Surveillance Technology Section (ESTS)
Operational Technology Division (OTD)
Hello,

There have been recent upgrades to Telephone Apps that allow the upload of data. The TS personnel in our office can now upload for the DCS3000 to TA directly. When these targets go Title III, we move the data to the VoiceBox and there is no current report which is compatible for upload to TA. I have tried to modify the current VoiceBox report with no luck. Do we know enough about the data that is captured by TA. Is there a plan to possibly have JSI create a report which can be uploaded to TA or will they have to continue to use hard copies of this data? This would be a great help to our folks here in Chicago.

Please let me know if I can be of any assistance.

Thanks,

ELSUR Technology Management Unit (ETMU)
Electronic Surveillance Technology Section, OTD
312 Desk
312 Fax
312 Cell
-----Original Message-----
From: [REDACTED]
Sent: Wednesday, May 18, 2005 10:41 AM
To: [REDACTED]
Subject: RE: Pen Register

This is a follow-up to the phone conversation that we had on June 2, 2005. I was wondering if you were able to agree on a meeting date. I will be on vacation on May 20, 2005 thru May 30, 2005. Could you tell me whether the CDNRS and J3094 data time are captures as real time or GMT? Will the contractor be able to add or use an existing field to the J3094 voice box file to indicate if a telephone number is

-----Original Message-----
From: [REDACTED]
Sent: Friday, May 06, 2005 9:28 AM
To: [REDACTED]
Subject: Pen Register

-----Original Message-----
From: [REDACTED]
Sent: Friday, April 15, 2005 8:57 AM
To: [REDACTED]
Subject: FW: Re current pen registers

-----Original Message-----
From: [REDACTED]
Sent: Thursday, February 20, 2003 9:48 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Re current pen registers
CM2210 (system no longer used) I am not sure if new format is used by another system.

ADNRS (system no longer used)

PCS (system no longer used)

'CDNRS (system no longer used) But, upload format used by DCS3000

RDNRS (no longer used)

JSI - what format is this?

DISCOVERY - not being used

J3094 - format being used

DCS - format being used

DMW - format being used

VOICE-ID - I did not know there was a format

PINE - (system no longer used)

NOKIA - I did not know there was a format

DCSPC - is this similar to DCS?

system being used; using DMW format

ICD-14 - format being used

Something to keep in mind .... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.
From: (OTD) (FBI)
Sent: Wednesday, October 05, 2005 8:05 AM
To: ICOTDHFBI)
Subject: RE: Pen Register

UNCLASSIFIED
NON-RECORD

Our vendor is in the process of rolling out an updated version of their application and we hope to start deploying this release in 2006. We will revisit the possibility of the [ ] option in that release.

---Original Message---
From: (ITOD)(CON)
Sent: Wednesday, October 05, 2005 8:05 AM
To: (OTD) (FBI)
Subject: RE: Pen Register

UNCLASSIFIED
NON-RECORD

This is a follow-up to the meeting you had with TA on June 1, 2005. I was wondering if the contractors working on the J3094 voice box file made any progress with adding or using an existing field to the J3094 voice box file to indicate if a telephone number is

---Original Message---
From: (ITOD)(CON)
Sent: Wednesday, May 18, 2005 10:41 AM
To: (OTD) (FBI)
Subject: RE: Pen Register

UNCLASSIFIED
NON-RECORD
This is a follow-up to the phone conversation that we had on June 2, 2005. I was wondering if you were able to agree on a meeting date. I will be on vacation on May 20, 2005 thru May 30, 2005. Could you tell me whether the CDNRS and J3094 data time are captured as real time or GMT? Will the contractor be able to add or use an existing field to the J3094 voice box file to indicate if a telephone number is

-----Original Message-----
From: [Name]  
Sent: Friday, May 06, 2005 9:28 AM  
To: [Name]  
Subject: Pen Register

UNCLASSIFIED
NON-RECORD

From: [Name]  
Sent: Friday, April 15, 2005 9:57 AM  
To: [Name]  
Subject: Fw: Re current pen registers

UNCLASSIFIED
NON-RECORD

CM2210 (system no longer used) I am not sure if new format is used by another system.  
ADNRS (system no longer used)  
PCS (system no longer used)  
CDNRS (system no longer used) But, upload format used by DCS3000  
RDNRS (no longer used)  
JSI - what format is this?
DISCOVERY - not being used  
J3094 - format being used  
DCS - format being used

(99)
DMW - format being used

VOICE-ID - I did not know there was a format

PINE - (system no longer used)

NOKIA - I did not know there was a format

DCSPC - is this similar to DCS?

stem being used; using DMW format

ICD-14 - format being used

Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.

Collection Management Unit (TICTU),
Electronic Surveillance Technology Section
Information Technology Division
ERF, Quantico, VA

Tel: 703
Fax: 703

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED
From: (OTD) (FBI)
Sent: Thursday, September 22, 2005 9:03 AM
To: (OTD) (CON)
Cc: (OTD) (FBI)
Subject: JOTD (FBI), 005

SENSITIVE BUT UNCLASSIFIED

I have copied a message from the TA company in New Orleans which will provide an update of their current situation:

Would ya'll forward this to whom ever you may think needs it, especially in the TICTU realm. Tomorrow, space management and FBI movers will commence moving all of our TA/ET/CMP equipment from New Orleans to our new offsite located at an undisclosed location. This includes moving all CMP equipment (Voice Box, DCS3000, etc.).

During this move I am sure things will be damaged. We cannot leave anything in place for space management is to begin gutting our entire field office next week. In a perfect world, we will be back in our New Orleans office by the end of May, or early June '06. In the interim our division will be scattered in bids from Covington, La to Baton Rouge, with Baton Rouge having several bids housing different programs. I have asked TICTU, et al to help set up temporary DCS 3000, etc in our current office. As far as any CMP down here, I do not know at this time how that will evolve, but once we get all equipment up here in BR, perhaps BAE could send some contractor types to check out all of our equipment. Also, I am sure we will have to surplus equipment but we will take it one step at a time.
Could you please tell me the status of the systems that are/were housed in the New Orleans FO? I was talking to [blank] (SMU) yesterday, and she told me the current building will be out of commission for at least 9-12 months, so I was wondering what has happened to these systems.

Regards,

ELSUR Technology Management Unit (ETMU)
Electronic Surveillance Technology Section, OTD
540 [blank] (Desk)
540 [blank] (Fax)
540 [blank] (Cell)
Greetings Gentlemen,

I hope you had a peaceful Memorial Day Weekend.

I have attached my list of Switch addresses. Could you please review for correctness? I know you are constantly updating and changing switch addresses.

I did not have anything loaded in the BQ Voice Box for ___________ and I was not sure if the ___________ was still good. I did input both and was successful in pinging both.

Based on the meetings last week, if I have either a ___________ I am under the impression that I need to set up two CDCs for any ___________ target. One CDC for ___________ data and one CDC for ___________ data.

If an ___________ target is using ___________ SSM network, do I also need to put the target up in a ___________ CDC?

The CMP has already ordered the RTF for the ___________ CALEA target. I have provided the CMP with the ring down number for the audio for the T-3. It is my understanding that the CMP will input the ___________ CALEA pen data into the DCS-3000. You will establish a new IP address and provide me with the IP address, port number, etc. that I need so I can get the pen data in the RAs for ___________ and Line CALEA.

I will be in the BQRA on Tuesday, but not at my desk. Please either call my cell phone 914 ___________ or page me at 888 ___________ (cell phone does not work well in Server room.)

Thank you

B6

B7C

SENSEI' BUT UNCLASSIFIED
This is a follow-up to the phone conversation that we had on June 2, 2005. I was wondering if you were able to agree on a meeting date. I will be on vacation on May 29, 2005 through May 30, 2005. Could you tell me whether the CDNRS and J3094 data time are captured as real time or GMT? Will the contractor be able to add or use an existing field to the J3094 voice box file to indicate if a telephone number is

-----Original Message-----
From: (ITOD)(CON)
Sent: Friday, May 06, 2005 9:28 AM
To: (ITOD)(CON)
Subject: Pen Register

UNCLASSIFIED
NON-RECORD

From: (ITOD)(CON)
Sent: Friday, April 15, 2005 9:57 AM
To: (ITOD)(CON)
Subject: FW: Re current pen registers

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: (ITOD)(CON)
Sent: Thursday, February 20, 2003 9:48 AM
To: 
Subject: Re: Re current pen registers

CM2210 (system no longer used) I am not sure if new format is used by another system.

ADNRS (system no longer used)
PCS (system no longer used)
CDNRS (system no longer used) But, upload format used by DCS3000
RDNRS (no longer used)
JSI - what format is this?
DISCOVERY - not being used
J3094 - format being used
DCS - format being used
DMW - format being used
VOICE-ID - I did not know there was a format
PINE - (system no longer used)
NOKIA - I did not know there was a format
DCSPC - is this similar to DCS?

system being used; using DMW format

ICD-14 - format being used

Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with All to discuss this and provide reports, files etc. for TA to decide how to handle.
From: (OTD) (FBI)  
Sent: Friday, May 06, 2005 9:28 AM  
To: ODT (FBI)  
Subject: Pen Register

UNCLASSIFIED  
NON-RECORD

From: (OTD) (CON)  
Sent: Friday, April 08, 2005 9:57 AM  
To: ODT (CON)  
Subject: FW: Re current pen registers

UNCLASSIFIED  
NON-RECORD

---- Original Message ----
From:  
Sent: Thursday, February 20, 2003 9:48 AM  
To:  
Cc:  
Subject: Re: Re current pen registers

CM2210 (system no longer used) I am not sure if new format is used by another system.
ADNRS (system no longer used)
PACS (system no longer used)
CDNRS (system no longer used) But, upload format used by DCS3000
RDNRS (no longer used)
JSI - what format is this?
DISCOVERY - not being used
J3094 - format being used
DCS - format being used
DMW - format being used
VOICE-ID - I did not know there was a format
PINE - (system no longer used)
NOKIA - I did not know there was a format
DCSPC - is this similar to DCS?

system being used; using DMW format

ICD-14 - format being used
Something to keep in mind ..... most of these formats need updating to include more fields of data that is being collected but unable to be passed to TA because TA database presently is not coded to handle. Have spoke to about this and it was decided that we should have a meeting with Ali to discuss this and provide reports, files etc. for TA to decide how to handle.

Telecommunications Intercept & Collection Management Unit (TICTU),
Electronic Surveillance Technology Section
Information Technology Division
ERF, Quantico, VA
Tel: 703
Fax: 703
I am verifying that you are the POC's for DCS 6000. Also, will you be available for a DOJCERT exercise the 20th and 21st of April?

Tks.

Intelligent Decisions, Inc.
FBI Enterprise Security Operations Center (ESOC)
Vulnerability Incident Assessment Cell (VIAC)
202
You are listed as a POC's for [redacted]. I need to know if this is still correct as we will soon need to correlate with you on a DOJCERT exercise.

Thanks.

Intelligent Decisions, Inc.
FBI Enterprise Security Operations Center (ESOC)
Vulnerability Incident Assessment Cell (VIAC)

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

(109)
Hello Guys,

Please review the following e-mail traffic. We will need to get involved sooner than later.

No, this is foolish! We [the SecD collective] have granted an ATO to the Program Managers/System Owners to manage their systems (DCS-XXXX) and we're not going to go back after the fact and ask for anything more...until either the ATO expires or they've demonstrated an inability to make sound risk decisions.

If AU wants to terminate their ATO(s) then I'll inform AD/ITD and SAC/CV of that decision.
I asked me to review the below thread and make a recommendation. After discussing with ..., here's what we came up with...

First, based on my recollection, the Voicebox is a portable system, but not necessarily a laptop. Second, since this Voicebox is NOT an FBI system that is being connected to an FBI system, it deserves some scrutiny from security, which I am sure that you have already done. We are assuming that this scenario may repeat itself in the future. Therefore, we feel that it would be appropriate for there to be a written operating procedure (most likely a page or two at most) that describes the following: 1) the Voicebox while attached to DCS 3000 will be under FBI control, 2) that appropriate safeguards are in place (listing safeguards), and 3) describing the sanitization process for ensuring that FBI data/information is not falling into the wrong hands when the Voicebox is removed from DCS 3000.

Once this is written and you review to ensure that it is adequate, we would ask that you please provide a copy of the operating procedure to the Accreditation Unit, so we can place it in the DCS 3000 C&A file for future reference. It would be the basis for future and similar request to do the same.

We did something similar to this (somewhat different circumstances) about 18 months ago involving a HIDTA operation in Denver. We agree that there is nothing here (at least on the surface) that would require any accreditation impact. We would just like it documented in the C&A file.

Hope this meets with your approval.

If you have any questions or would like to discuss, please let me know.

Thanks!

Are you aware of the attached proposal to connect laptops to DCS 3000? I asked if it changed the accreditation boundary - I would think there is a good chance it does.
This DCS thing has tentacles. I have assigned this to How did you respond to

---Original Message---
From: (SecD) (FBI)
Sent: Thursday, February 03, 2005 9:20 AM
To: (SecD) (FBI)
Cc: (SecD)(CON)
Subject: FW: Portable Voicebox

---Original Message---
From: (CV) (FBI)
Sent: Thursday, February 03, 2005 9:16 AM
To: [CV] (FBI);[CV](CON); (SecD)(CON);
Cc: (CV) (FBI);(CV) (FBI);(CV) (FBI);
Subject: RE: Portable Voicebox

---Original Message---
From: (CV) (FBI)
Sent: Wednesday, February 02, 2005 4:29 PM
To: [CV] (FBI);
Cc: [CV] (CON); [CV] (FBI);
Subject: Portable Voicebox

Hi will be happy to assist you in this matter. Sending you to the experts:-) Take care...
Several months ago, I spoke to you regarding our task force squad that purchased its own Voicebox digital collection system and needed the OK from Security Division to use it on FBI cases. This is still in the works on our end, but we have a similar situation regarding a portable system and require the input of Security Division before we move forward.

Quantico ERF has supplied our division with a portable Voicebox system, but it is currently in use in our Toledo RA. The case agent in our Youngstown RA would like to conduct an upcoming FBI T-III on a digital system (rather than cassette tapes), but we do not have another system available (niether does ERF). The local HIDTA has purchased a portable Voicebox system and has agreed to let the Youngstown RA use it for this T-III. The system will be operated in the RA space and would be connected to our DCS-3000 network to obtain telephone target data. According to ERF, there is an acceptable configuration which enables secure transfer of the data. The issue arises in regards to conducting an FBI case on a system that is not owned by the FBI. As far as the data and audio that will be stored on the system is concerned, if necessary, we could remove the hard drives from the system before it is returned to HIDTA (replacements would have to be supplied by the FBI and software reloaded by the manufacturer).

From the security standpoint, can we use this system to conduct this upcoming T-III? Are there any other issues that must be resolved?

If you have any questions, please feel free to call me.

Thanks,

Cleveland Division
21 Office
21 Cell

(116)
This is my response to:

--- Original Message ---

From: [Redacted]
Sent: Thursday, January 13, 2005 1:51 PM
To: [Redacted]
Cc: [Redacted]
Subject: [Redacted]

I got your name through [Redacted] he said you may be able to help me answer some questions I have about [Redacted] all I need is contact information for the system administrator, the ISSO, and the ISSM.

I am our System Administrator, I am the ISSO and [Redacted] is the ISSM for the [Redacted] project.

Also, I need to know which network [Redacted] resides on.

The [Redacted] is a self contained Windows domain network which functions as a tool for telecommunication interception used in Title III case work. The systems are developed and provided by a contracted vendor which specializes in this type of investigative tool. Each field office has a version of this network in place (varying in size according to need). Additionally a number of RAs have a system. The combination of these systems is reaching 100. The systems do have a firewalled link to the DCS3000 project which allows the systems to receive the Call Data Content record information from wireless technology intercepted calls. The systems run at the sensitive but unclassified level.
From: (OTD) (FBI)  
Sent: Tuesday, January 18, 2005 8:42 AM  
To: (ITD) (FBI)  
Subject: FW:

---Original Message---
From: (ITD) (FBI)  
Sent: Thursday, January 13, 2005 1:51 PM  
To: (SecD) (CON)  
Cc: (ITD) (FBI)  
Subject:  

I forwarded this message to me.  

I got your name through [redacted] he said you may be able to help me answer some questions I have about [redacted]. I need contact information for the system administrator, the ISSO, and the ISSM.  

[redacted] is our system administrator, I am the ISSO and [redacted] is the ISSM for the [redacted] project.  

Also, I need to know which network besides [redacted].  

[redacted] is a self contained Windows domain network [redacted] the systems are developed and provided by a contracted vendor which specializes in this type of investigative tool. Each field office has a version of this network in place [redacted] The systems do have a firewalled link to the DCS3000 project which allows the systems to receive the
Hello Guys,

Here is an e-mail moving about regarding C & A.

Please review.

FYI...if there is any reason(s) not to...please advise.
Gents,

After many internal discussion regarding the Certification and Accreditation (C&A) process of systems, we [AU, CU, and I] came to the conclusion that combining systems under one C&A makes sense (in some cases). I'd like to get your opinion on this matter as I'm looking to combine the collections systems (DCSnet, DCS 3000, 5000, 6000, and J3094) under one C&A (if that makes sense to do so).

I'd like to arrange a meeting for 13:30 tomorrow 19 January to discuss and collect your comments. We can meet in my office unless someone has a better alternative.
From: [redacted]
Sent: Thursday, January 13, 2005 1:51 PM
To: [redacted]
Cc: [redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I forwarded this message to me.

I got your name through [redacted]. He said you may be able to help me answer some questions I have about [redacted]. All I need is contact information for the system administrator, the ISSO, and the ISSM.

As our System Administrator, I am the ISSO and [redacted] is the ISSM for the [redacted] project.

Also, I need to know which network [redacted] resides on.

The [redacted] is a self-contained Windows domain network which [redacted]. The systems are developed and provided by a contracted vendor which specializes in this type of investigative tool. Each field office has a version of this network in place. The systems do have a firewall link to the DCS3000 project which allows the systems to receive the...

703 [redacted]
From: (ITD) (FBI)
Sent: Thursday, January 13, 2005 1:51 PM
To: (SecD) (CON)
Cc: (ITD) (FBI)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

forwarded this message to me.

I got your name through he said you may be able to help me answer some questions I have about need is contact information for the system administrator, the ISSO, and the ISSM.

is our System Administrator, I am the ISSO and is the ISSM for the project.

Also, I need to know which network resides on.

The is a self contained Windows domain network which functions as a tool for telecommunication interception used in Title III case work. The systems are developed and provided by a contracted vendor which specializes in this type of investigative tool. Each field office has a version of this network in place (varying in size according to need). Additionally a number of RAs have a system. The combination of these systems is reaching 100. The systems do have a firewalled link to the DCS3000 project which allows the systems to receive the Cali Data Content record information from wireless technology intercepted calls. The systems run at the sensitive but unclassified level.
Sensitivity: SENSITIVE BUT UNCLASSIFIED  
Non-record: NON-RECORD  

Response to DCS6000 security inquiry

The following actions should be completed by ITD:

C Establish and document standard physical access requirements for deployed systems within 90 days.

Each fielded system is being updated with the proper security features. This requires an onsite visit by the vendor representative to be implemented, which requires a coordination of schedules of Vendor and office personnel. If current Title III collections are ongoing then this requires after-hours scheduling. We have moved from 25% in July to 80% complete at this time. Our goal is to complete this process by March 31, 2005.

C Implement formal Change Management. In the interim, ensure all sites have an emergency repair disk that reflects the original configuration in addition to backup tapes.

The Change Management issue has been brought up to the vendor as a necessary of our security requirements. All changes to the systems come from the vendor and we are currently two software revisions below their current implementations. The vendor will start providing the process in the newer version. We have not moved to the newer software version due to the strain of maintaining the requirements of the accreditation process and the time that it takes to implement the changes throughout our environment. We will be looking at moving forward in the last half of FY05.

The vendor has a system of RAIDS and backups to opposite machines within the network for restoration operation. If a system must be restored, then the system must be returned to ERF for repair or a Vendor representative sent onsite. No tape backups are used, evidence that may be used for a case is stored in real-time on a pair of magneto optical disc. In the next version of software offline backup of software will be implemented.

C Implement a weekly security review to existing audit procedures. The Program Manager and/or the ISSO should review the Rules of Behavior and maintain signed copies for all users within 90 days.

Each system that has been updated has received a notebook detailing the SSP and associated documents. Rules of Behavior forms are included for privilege and general users. This notebook details procedures and responsibilities of on-site administrators and security personnel. The vendors procedures for managing audit logs is inconsistent and this issue has been brought up to them. They are working on correcting this issue, once the issue is resolved and implemented the procedures for reviewing and maintaining the audit logs will be standardized for field personnel.

The DCS3000, DCS5000 and DCS6000 are anticipated to merge into a network and will require a new C&A.
The DCS-6000 is currently accesses the DCS-3000 network for CDC call information. Each DCS-6000 network system requires a CISCO PIX firewall between itself and the DCS-3000. This firewall is strictly configured to allow only desired traffic to the designated machines within the DCS-6000 network.

The Information Technology Security Unit (ITSU) will provide verification to the AU of these actions in certification documents for the resulting new system. Maintaining a current accreditation status is subject to the continued adherence to the provisions of the SSP. In particular, all media copied or downloaded from the DCS6000 must be scanned for malicious code with the latest available virus scan updates before introducing information to any application residing on the FBI LAN/WAN.

- It is our intention to begin the reworking of the SSP at the beginning of 2005 to conform to our operational requirements for the DCS-6000.
- Over 90% of the DCS-6000 system are running McAfee anti-virus software with 100% anticipated by completion of system updates in March of 2005.
- At this time there is only one text file of data that may be exported for transfer over to the FBI/WAN by diskette for upload into an application. Less than 20% of offices use this feature and they are required by standard operating procedures to scan this file before proceeding.

SENSITIVE BUT UNCLASSIFIED.
FW: DCS 6000

I currently have [REDACTED] as the ISSO for the DCS 6000. Just as with the DCS 3000 I am now having to follow up with the progress of the action plan for the DCS 6000. Attached is the EC which identifies the things that are supposed to be addressed. Could you work with the owners to determine if any of the items have been addressed, and if none, provide projected dates.

Respectfully,

[REDACTED]

AU, IAS, Security Division
(202) [REDACTED]
On the last trip up to Anchorage they wanted to test audio coming from ACS. The audio was fine but the call would not disconnect, had to manually disconnect the line. If you left the line open it actually would disconnect (it took about 1-2 minutes after the target went on hook). Is there anything that can be done for this I know it is a known issue but is it being looked at to see if it can be corrected.

Also they were trying to get their VoiceBox to except the digit info from the DCS3000 but I needed the info to put in the screen (IP address and port).

Thank you

Electronic Surveillance Operations Support Office (EOSO)
Electronic Surveillance Technology Section (ESTS)
Investigative Technology Division (ITD)
206 (Desk)
206 (Cell)
206 (Fax)
Some time ago I approached you, via an e-mail, regarding combining the ATO's for the DCS-family of computers (3000, 5000, 6000, DCSnet and J3094). You indicated that you'd like to get together to discuss the Tiers and LOC's for these systems, ultimately to determine if joining them made sense. I haven't heard from you, so I thought I'd send a follow-up note to ask about your progress. When do you want to meet?

Cheers

ISSM, Quantico Complex
ERF (703)
Im back this week, please call or stop by when you get a chance.

--- Original Message ---

Good Morning

In regard to the Security issues that we discussed, please find a draft of the General User Rules of Behavior attached. I am still working the issue regarding the "Mission Exception" statement for a Task force.

As far as the connection to the DCS-3000, I am working with The SSP will have to be updated and put into the right format. Depending on the Levels of Concerns for the DCS-3000 and DCS-6000 and all of its external connections, the C&A or part of the C&A will have to be revalidated.

We are currently waiting on information for the DCS-3000 and DCSNet.

V/R
Good Morning

In regard to the Security issues that we discussed, please find a draft of the General User Rules of Behavior attached. I am still working the issue regarding the "Mission Exception" statement for a Task force.

As far as the connection to the DCS-3000, I am working with [redacted]. The SSP will have to be updated and put into the right format. Depending on the Levels of Concerns for the DCS-3000 and DCS-6000 and all of its external connections, the C&A or part of the C&A will have to be revalidated.

We are currently waiting on information for the DCS-3000 and DCSNet.

V/R

SENSITIVE BUT UNCLASSIFIED
The DCS3000 column was in my mind to indicate connectivity between the DCS3000 and VoiceBox. I believe that most portables do not have the PIX to make that happen. Perhaps other systems out there are still without that connectivity as well.

That will be fine.

The notebook column is for a notebook that I am preparing for all sites that will include security information and procedure guides and other items for the VoiceBox system. I am working on putting one together and need to fine tune it before issuing it to the field.

I thought of putting a Version Number column at first but I didn't have all that info so I was just going to use the Yes/No choice to designate the systems that I knew were upgraded, but if your guys can fill in all that info with the current version number then that will be great.

What would be in the DCS3000 column, I know all division offices have connectivity and most RAs?
and the Virus protection installed I think that it is valid. I think also that instead of the VB Updated column title that Version Number would work better.

I am curious what the Notebook Provided column is about. And I am guessing that the Schedule Date and Complete Date are for scheduling upgrades and new installs and to record what it actually slips to.

If you agree to the changes that I suggested I will forward this to the regional managers tomorrow.
could you have your guys also verify the information in the VB System Type column for correctness.

Thanks

-----Original Message-----
From: (ITD) (CON)  
Sent: Tuesday, August 10, 2004 7:13 PM  
To: (ITD) (FBI)  
Subject: RE: Spreadsheet

I am adding another column to your spreadsheet for DCS3000 connectivity. Since that is key to getting PEN data and the Virus protection installed I think that it is valid. I think also that instead of the VB Updated column title that Version Number would work better.

I am curious what the Notebook Provided column is about. And I am guessing that the Schedule Date and Complete Date are for scheduling upgrades and new installs and to record what it actually slips to.

If you agree to the changes that I suggested I will forward this to the regional managers tomorrow.
UNCLASSIFIED
NON-RECORD

That will be fine.

The notebook column is for a notebook that I am preparing for all sites that will include security information and procedure guides and other items for the VoiceBox system. I am working on putting one together and need to fine tune it before issuing it to the field.

I thought of putting a Version Number column at first but I didn't have all that info so I was just going to use the Yes/No choice to designate the systems that I knew were upgraded, but if your guys can fill in all that info with the current version number then that will be great.

What would be in the DCS3000 column, I know all division offices have connectivity and most RAs?

---Original Message---
From: (ITD) (FBI)
Sent: Tuesday, August 10, 2004 7:13 PM
To: (ITD) (CON)
Subject: RE: Spreadsheet

UNCLASSIFIED
NON-RECORD

I am adding another column to your spreadsheet for DCS3000 connectivity. Since that is key to getting PEN data and the Virus protection installed I think that it is valid. I think also that instead of the VB Updated column title that Version Number would work better.

I am curious what the Notebook Provided column is about. And I am guessing that the Schedule Date and Complete Date are for scheduling upgrades and new installs and to record what it actually slips to.

If you agree to the changes that I suggested I will forward this to the regional managers tomorrow.

---Original Message---
From: (ITD) (FBI)
Sent: Tuesday, August 10, 2004 11:23 AM
To: (ITD) (CON)
Subject: Spreadsheet

UNCLASSIFIED
SECRET (136)
I am adding another column to your spreadsheet for DCS3000 connectivity. Since that is key to getting PEN data and the Virus protection installed I think that it is valid. I think also that instead of the VB Updated column title that Version Number would work better.

I am curious what the Notebook Provided column is about. And I am guessing that the Schedule Date and Complete Date are for scheduling upgrades and new installs and to record what it actually slips to.

If you agree to the changes that I suggested I will forward this to the regional managers tomorrow.
IOTP) (FBI)

--- Original Message ---
From: (ITD) (FBI)
Sent: Tuesday, August 03, 2004 4:27 PM
To: (ITD) (FBI)
Cc: (ITD) (FBI)
Subject: RE: Virus Scan Installation Instructions for Voicebox Fixed Site Systems

UNCLASSIFIED
NON-RECORD

Have we completed this? Please provide a status.

--- Original Message ---
From: (ITD) (FBI)
Sent: Monday, July 19, 2004 12:05 PM
To: (ITD) (FBI)
Cc: (ITD) (FBI)
Subject: RE: Virus Scan Installation Instructions for Voicebox Fixed Site Systems

UNCLASSIFIED
NON-RECORD

No, I just heard of it. I will get on it.

Please see that this is done in the field. Please keep track of when all sites are complete and email that back to me. Set a deadline of by the end of the month. If deadline cannot be met I want to know why. Thanks.

--- Original Message ---
From: (ITD) (FBI)
Sent: Monday, July 19, 2004 11:24 AM
To: (ITD) (FBI)
Cc: (ITD) (FBI)
Subject: FW: Virus Scan Installation Instructions for Voicebox Fixed Site Systems

UNCLASSIFIED
NON-RECORD
Have we done this yet?

--- Original Message ---

From: (ITD) (FBI)
Sent: Thursday, July 08, 2004 11:48 AM
To: (ITD) (FBI)
Subject: FW: Virus Scan Installation Instructions for Voicebox Fixed Site Systems

UNCLASSIFIED
NON-RECORD

Hey —

Please distribute this information to the field — for DCSP distribution. Thanks.

--- Original Message ---

From: (ITD) (FBI)
Sent: Thursday, July 08, 2004 9:50 AM
To: (ITD) (FBI)
Subject: Virus Scan Installation Instructions for Voicebox Fixed Site Systems

UNCLASSIFIED
NON-RECORD

Due to the Certification & Accreditation of the Voicebox System, its mandated that all VoiceBox workstations have Virus Scan software loaded and running. The attached file contains instructions for installation and setup on the Virus Scan software. The Virus Scan Software should be installed as soon as possible. When completed you must email — to inform him that virus scan is installed and running.

Your VoiceBox system must have a connection to the DCS network. This connection will allow your system to connect to the DCS 3000 Web page on the machine. The Web page contains downloads for McAfee Virus Scan (for workstations running Windows 2000 Professional) and Netshield (for Windows 2000 Server). The connection will also allow the Virus Scan software to update automatically.

If you have questions please contact:

If you could send this to — to request that the DCSP personnel in the field could perform this task.

Thank you
### DCS 3000 Switch Addresses

<table>
<thead>
<tr>
<th>Local Port</th>
<th>Remote Port</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5001</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5000</td>
<td></td>
</tr>
</tbody>
</table>

### Port

<table>
<thead>
<tr>
<th>Location</th>
<th>ISG-1</th>
<th>ISG-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elmsford ISG</td>
<td>6195</td>
<td></td>
</tr>
<tr>
<td>Boston/New England</td>
<td>6195</td>
<td></td>
</tr>
<tr>
<td>Los Angeles/Las Vegas</td>
<td>6195</td>
<td></td>
</tr>
</tbody>
</table>

Southern California is the Los Angeles Vanguard and covers Las Vegas, Nevada.

---

#1056782-000