Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CDs

Section: 6

Federal Bureau of Investigation

Goals and Objectives

b6
b7C

Electronics Engineer

Purpose

Goals and Objectives

The ISTIC is an introductory course on CALEA intercept techniques and procedures. Upon completion of this course students should have a basic understanding of the CALEA Paradigm and specific training on the implementation of CALEA pen register collections utilizing the DCS 3000 suite of applications.

Background

Goals and Objectives

The Switch Based Intercept Team is responsible for the development, deployment and maintenance of telephone switch-based ELSUR capabilities

DCS 3000 is the current interim solution used by the FBI

The FBI is investigating and deploying other options from outside vendors

Goals and Objectives

Educate TTAs on:

- **Technologies utilized, FBI equipment needed, connection information for service providers, DCS 3000 application hardware, operating system, and infrastructure needed for implementation and maintenance**
- **Current issues affecting ELSUR operations**

Enable "graduates" to implement and maintain switch based intercepts in their field divisions with specific training on the DCS 3000 system

Interim Solutions For Telecommunications Intercepts Course

Engineering Research Facility
Quantico, Virginia

August 10 - 19, 2004

PURPOSE: This course is designed to reduce the demands placed on TICTU by establishing a cadre of interim solutions subject matter experts

---

BACKGROUND:

- TICTU responsibilities include the development, deployment and support of advanced interception applications to FBI field office throughout the country.
- TICTU has provided similar support, on request, to other federal, state and local agencies
- DCS-3000 is the current interim solution used by the FBI as the FBI continues to investigate other options.

DILEMMA:

- There has been an increase in requests for assistance from agencies outside the FBI due to the increasing popularity of PCS service in the United States.
- The volume of support requests threaten to interfere with the primary functions of TICTU:
  - Providing support to bureau field offices, and
  - Conducting R&D to keep pace with evolving technologies

COURSE GOALS AND OBJECTIVES:

- This course was designed to help reduce the number of request for assistance, thereby allowing TICTI to concentrate on its primary responsibilities
- This course will provide information on:
  - Personal Communications Services
  - Technologies utilized by service providers
  - All aspects of the DCS-3000 application, including the hardware, operating system and infrastructure necessary to deploy and maintain it
  - Current issues affecting ELSUR operations
- "Graduates" will be able to fully support their own DCS-3000 installations
- Attendees may be called upon to train counterparts in neighboring and/or related agencies in subsequent DCS-3000 deployments. Demands will be reasonable
- Only through this educational approach can TICTU continue to provide the level of technical assistance requested by agencies outside the FBI

ELSUR / Service Provider Cooperation

b6
b7C

Senior Consultant

Switch Based Intercept Team Web Site on LEO

ELSUR / Service Provider Cooperation

Special Interest Groups

LEOSIGs | TICTU | Member Area

ELEVATED

Telecommunications Intercept and Collection Technology Unit

FBI Intelligence Information & Products

Open to LESC Members Only

Member Area

- Address Book
- Calendar
  - Contribute to TICTU Calendar
- ERF Contacts
- Links
- News
- Resources
- Training

b6
b7C

News

- Get the lates[redacted]nformation in the Carrier Data section.
- For upgraded DCS-3000 software, please contac[redacted]
- DCS 3000 Manual and Release Notes updated in the Resources section: October 29, 2002.
- ERF Contacts List updated: October 29, 2002
- Training dates updated: October 29, 2002

b2
b7E

Tech Alert 040528

The Microsoft Service Pack 2 Beta for Windows XP offers enhanced [illegible]ity features that caus[illegible]lems accessing [illegible]EO secure website.

In an effort to prevent this issue, LEO members are encouraged NOT to install Service Pack 2 on any systems used to access LEO

Switch Based Intercept Team Web Site on LEO

(Continued)

Resources

- **DCS-3000**
  - **Manual**
  - **Release Notes**
- **Reference Materials**
  - **Carrier-Specific ELSUR Material**
    - **LER Guides/POC Information**
    - **CALEA Worksheets/Fax Coversheets**
  - **CALEA Data**
  - **FCC License Information**
  - **Course Materials**
    - **ISTIC**
    - **Regional Training Seminars**

Packet Assembler / Disassember

b6
b7C

Electronics Technician

Packet Assembler / Disassembler

Packet Assembler / Disassember

b2
b7E

CALL DATA CHANNEL

CALL CONTENT CHANNEL

NORTEL DMS – 100/500/MTX
CDC Delivery

b2
b7E

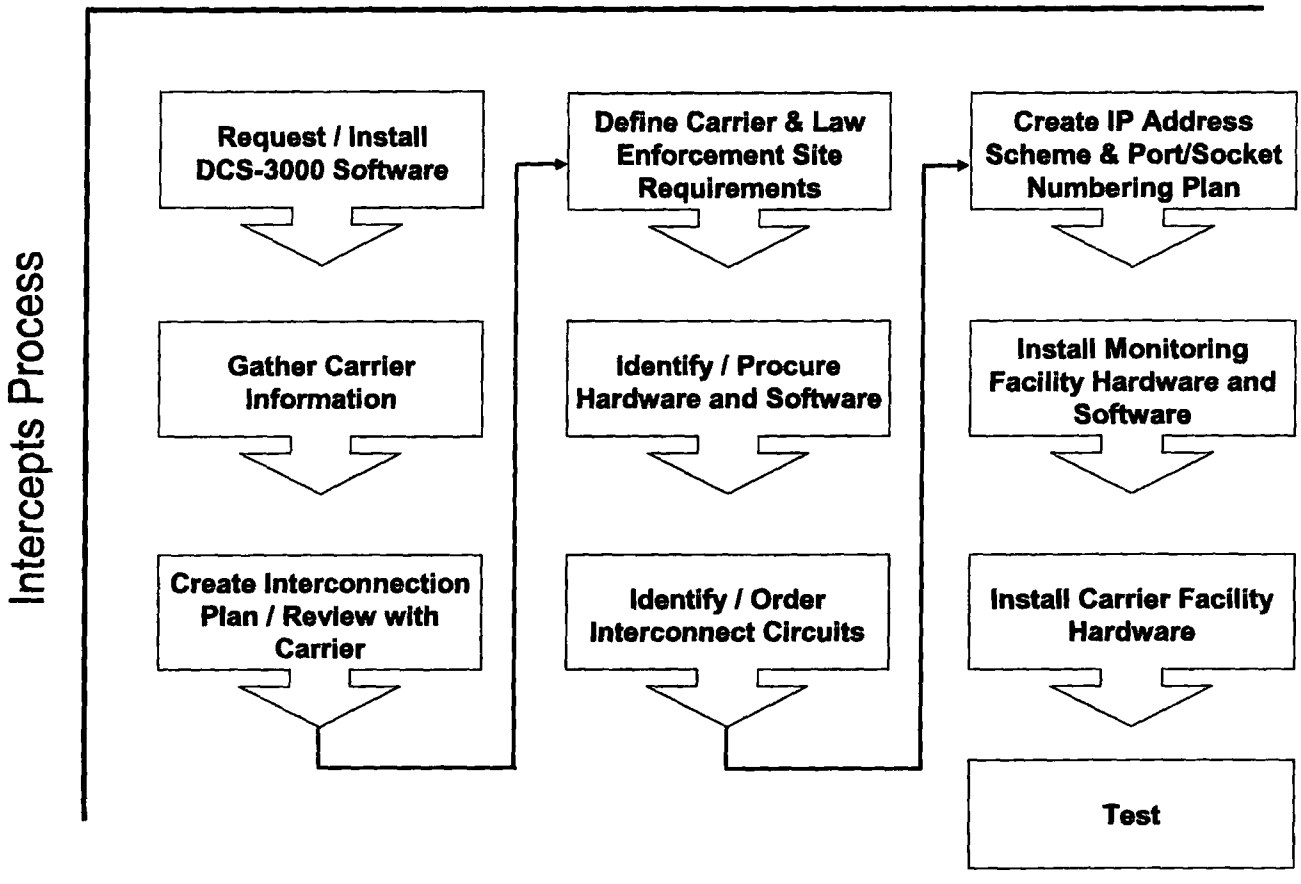
Intercepts Process

b6
b7C

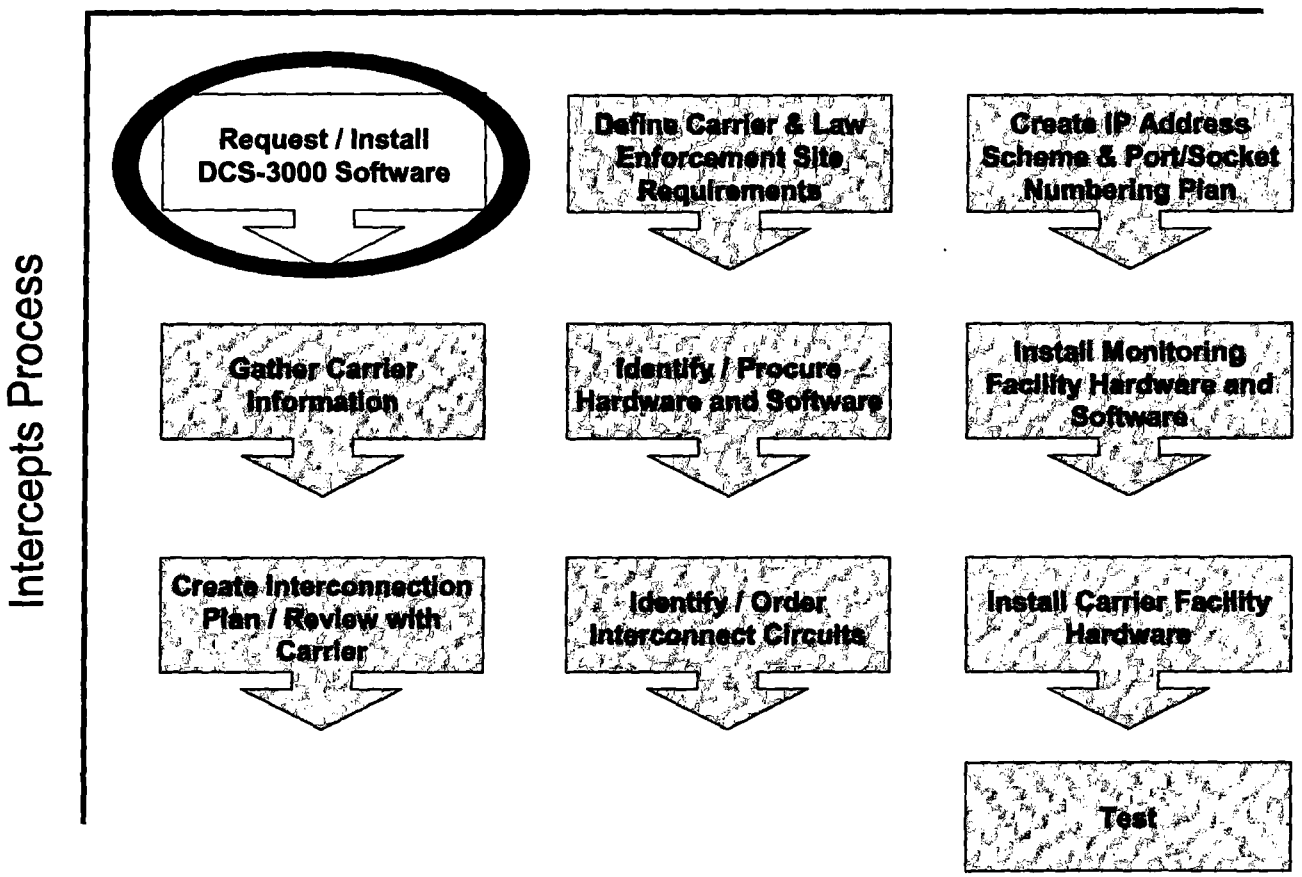
[redacted]

Senior Consultant

FBI Overview



Intercepts Process

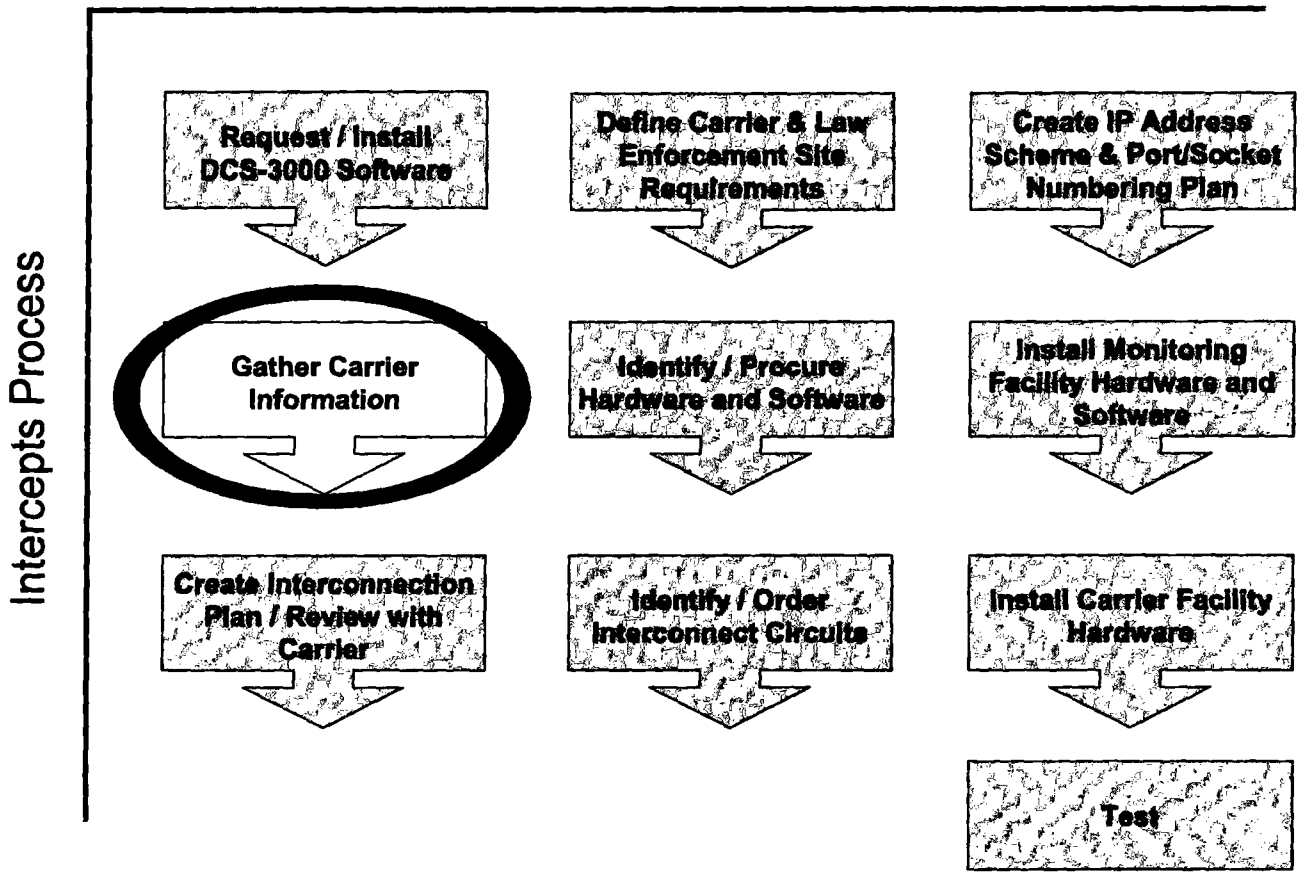


Request/Install DCS-3000 Software

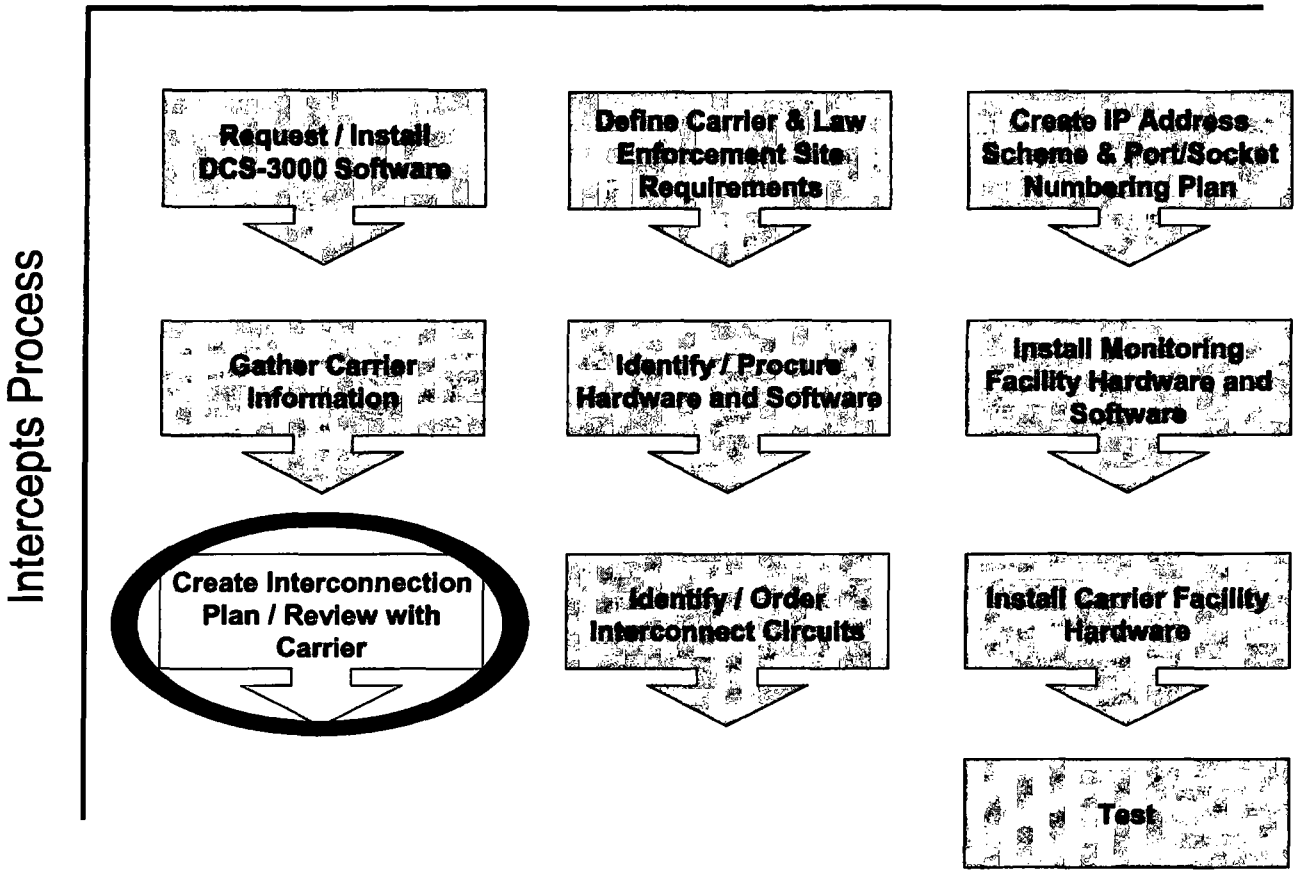
Intercepts Process

- **Request current copy of DCS-3000 software from ERF**
- **Follow authentication procedures to install software**

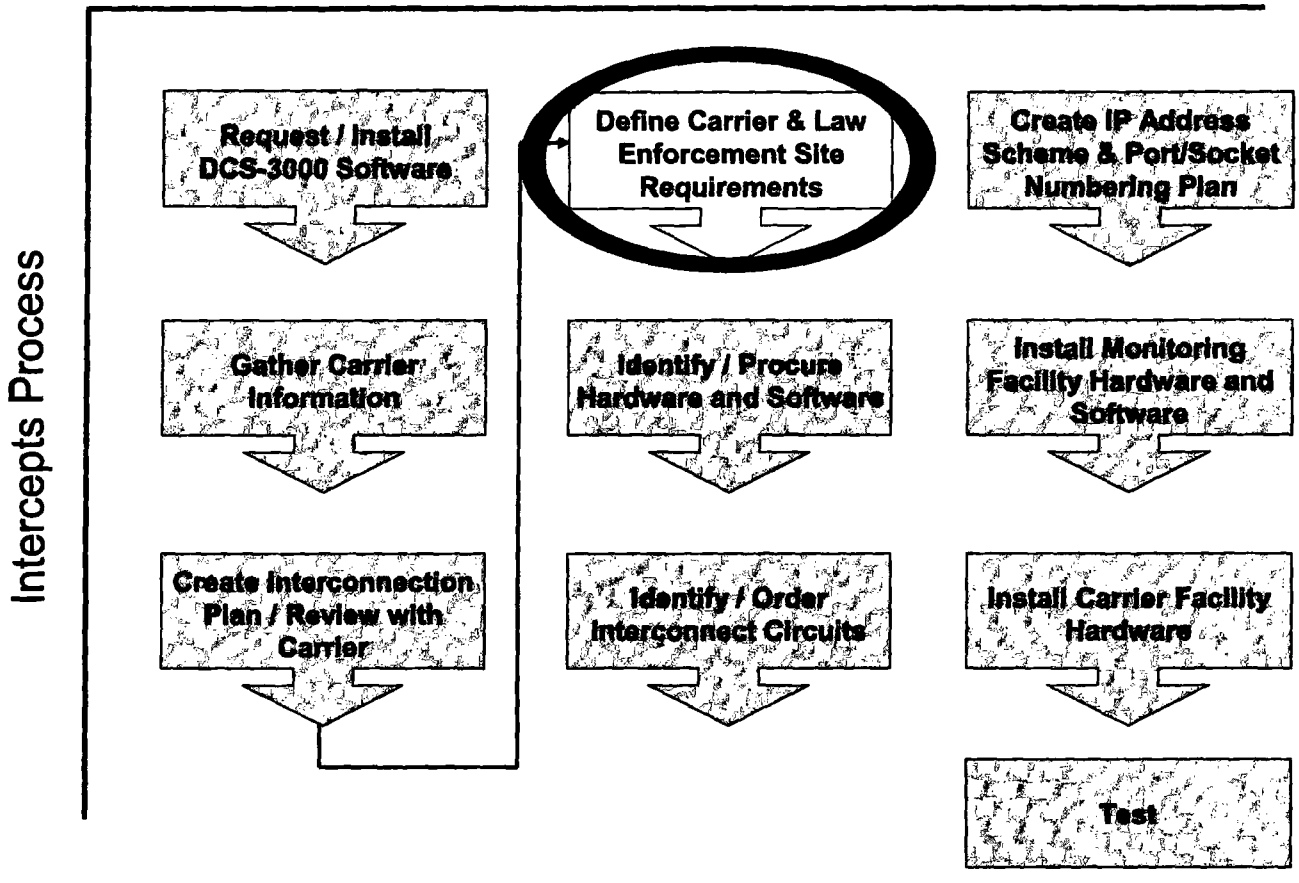
Intercepts Process



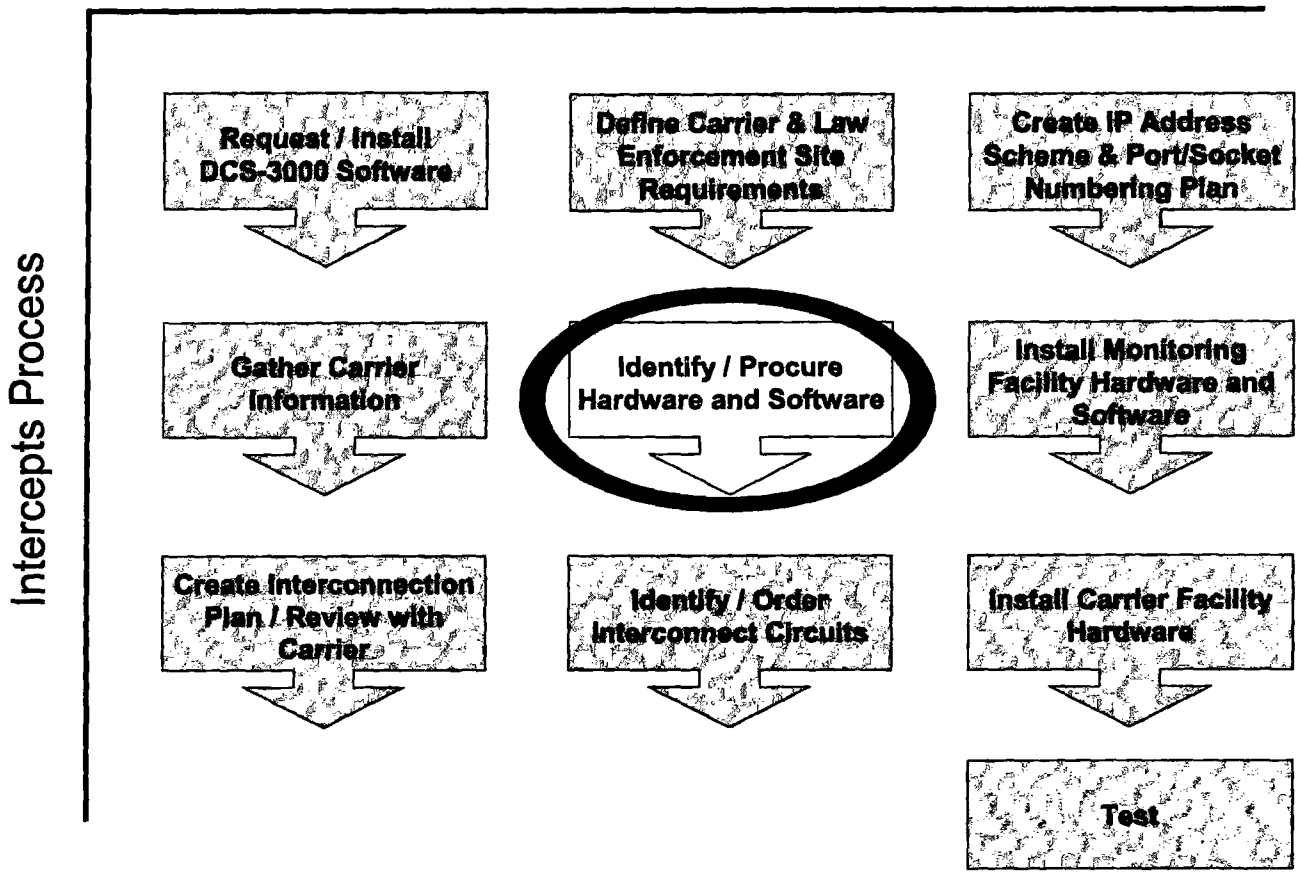
Intercepts Process



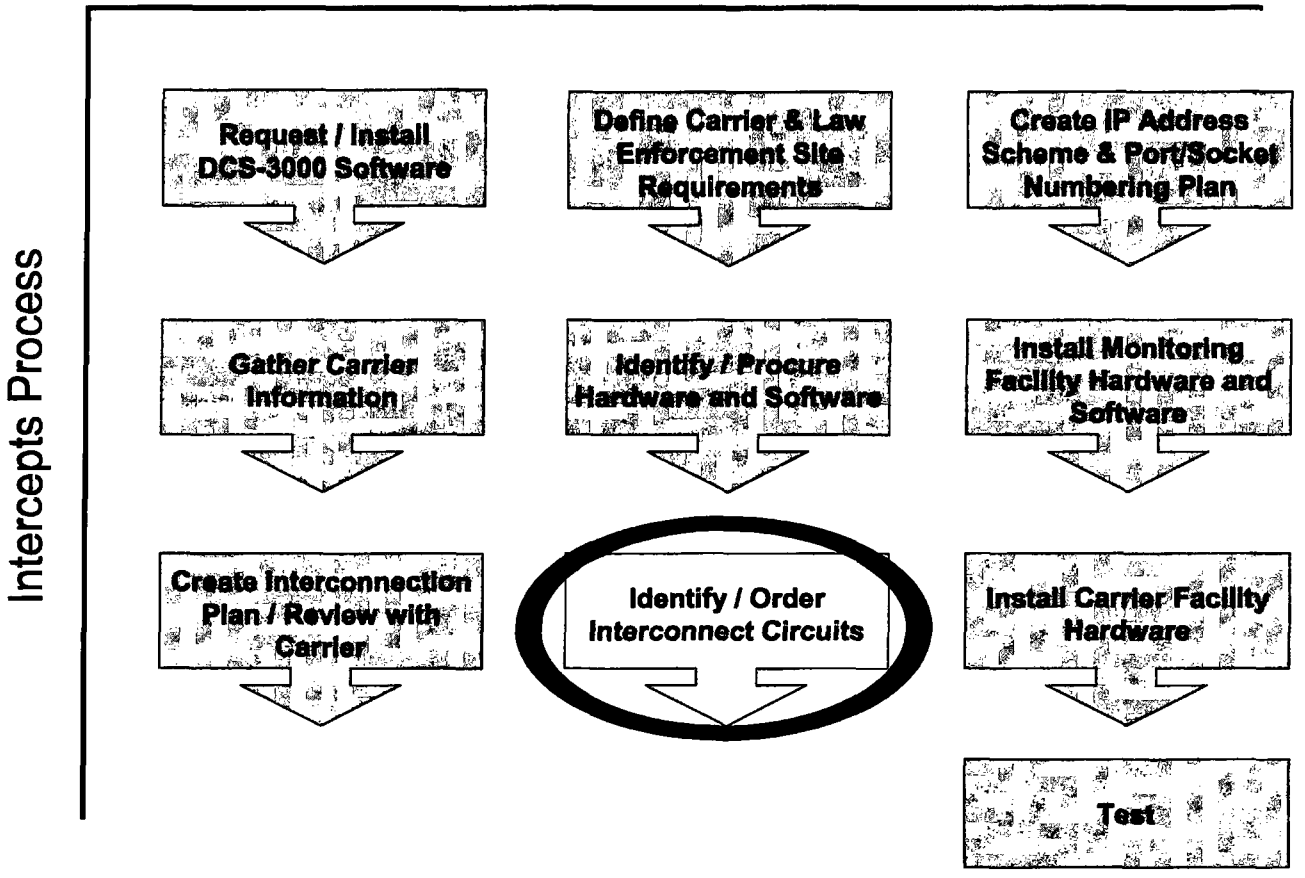
Intercepts Process



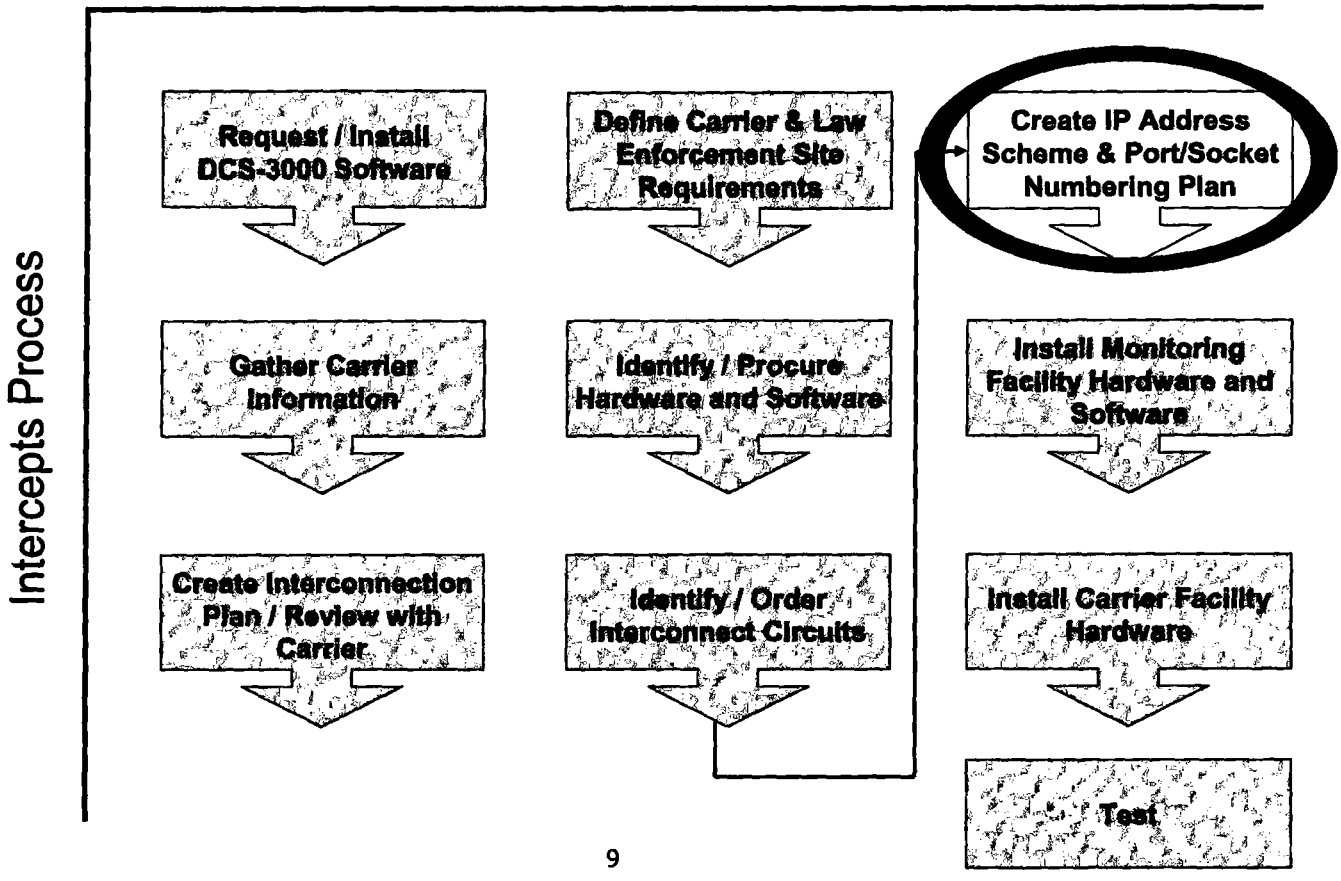
Intercepts Process



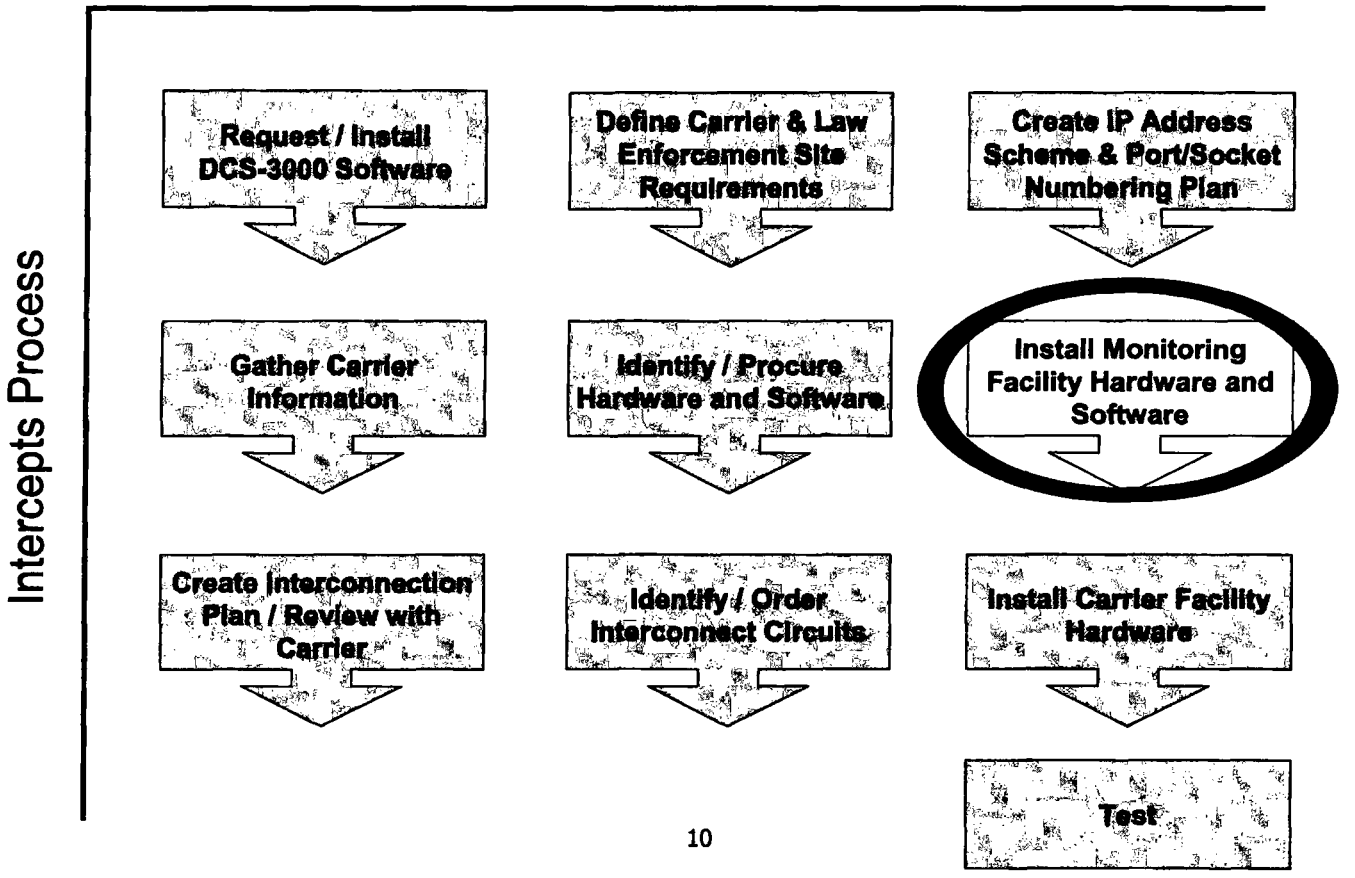
Intercepts Process



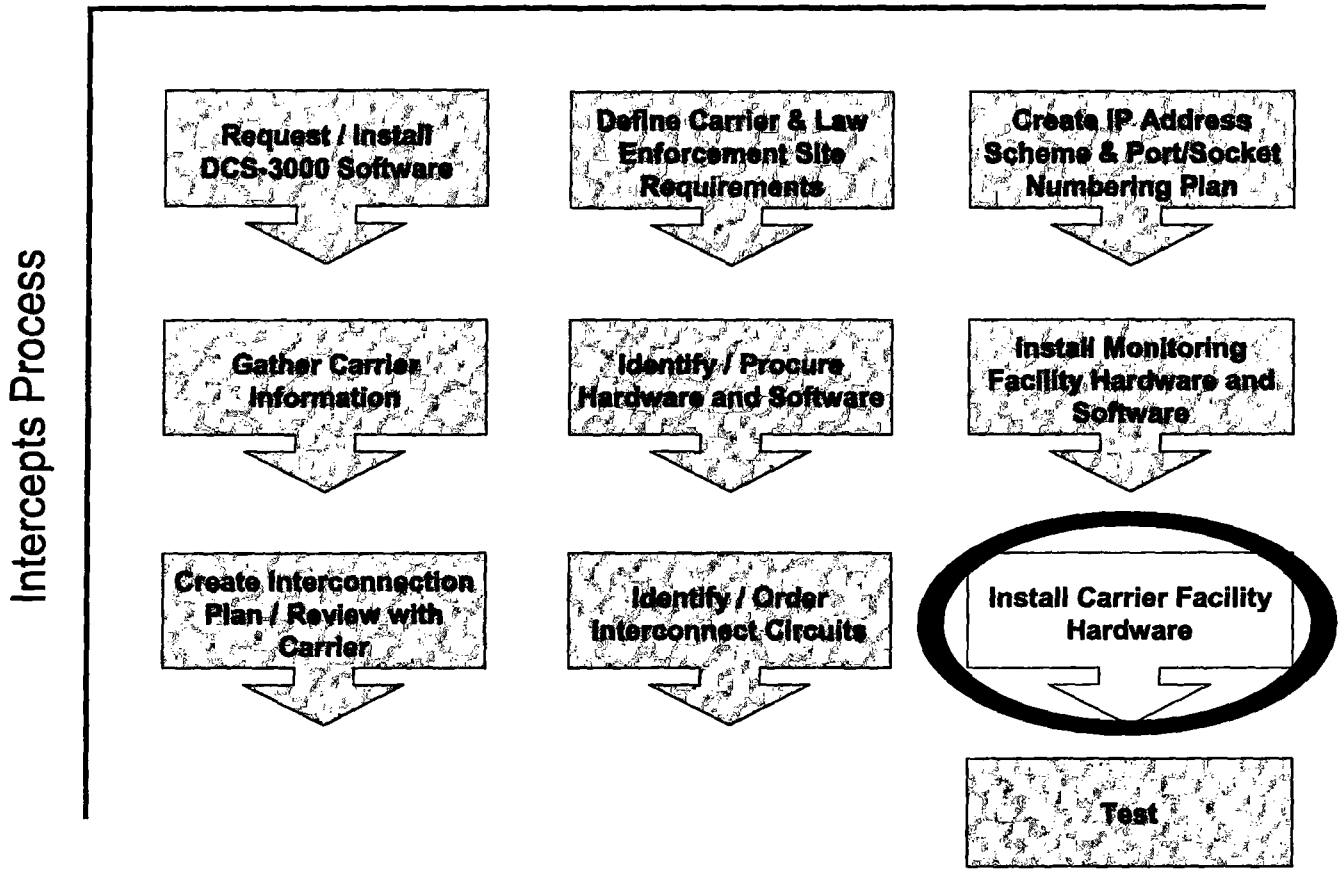
Intercepts Process



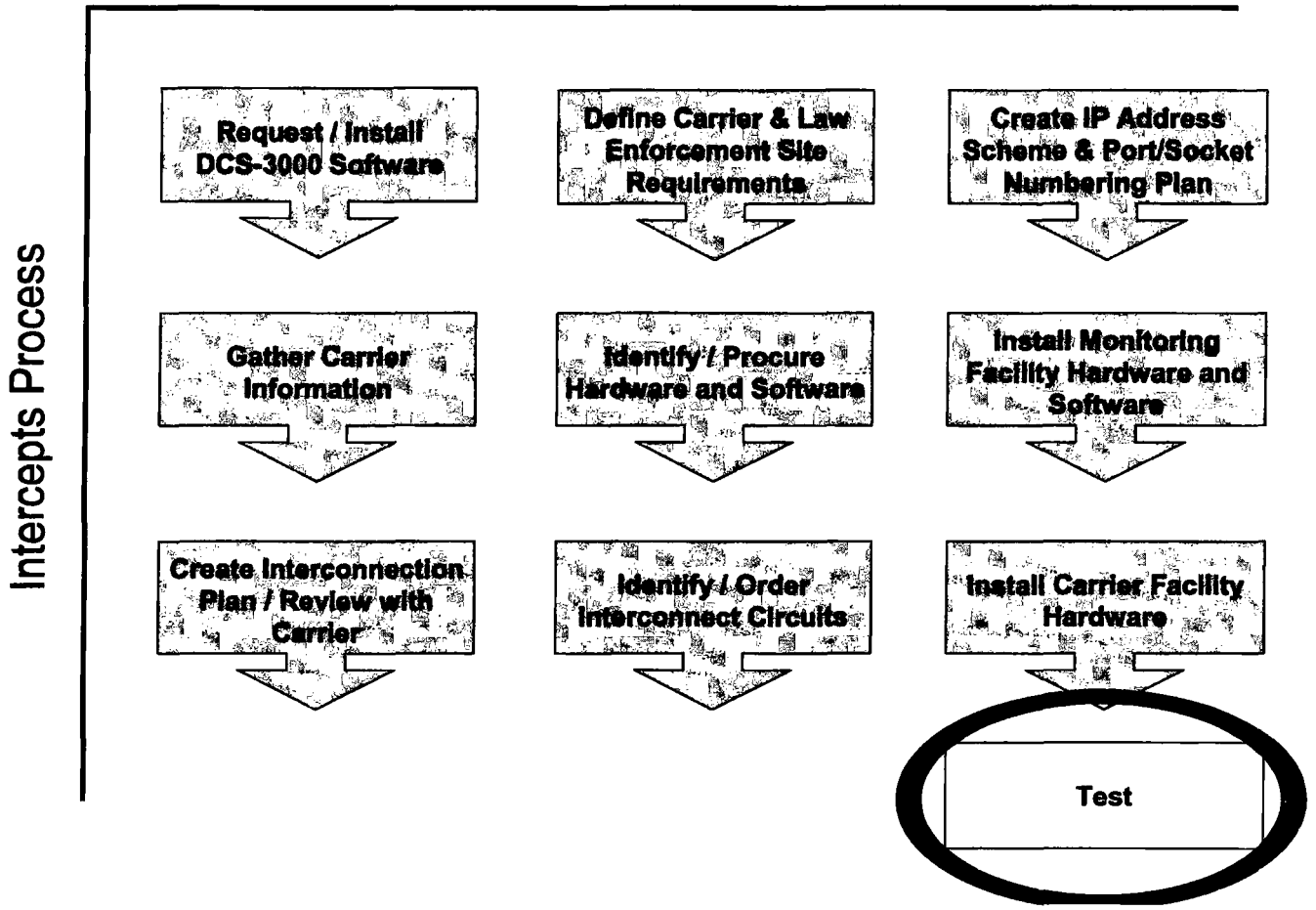
Intercepts Process



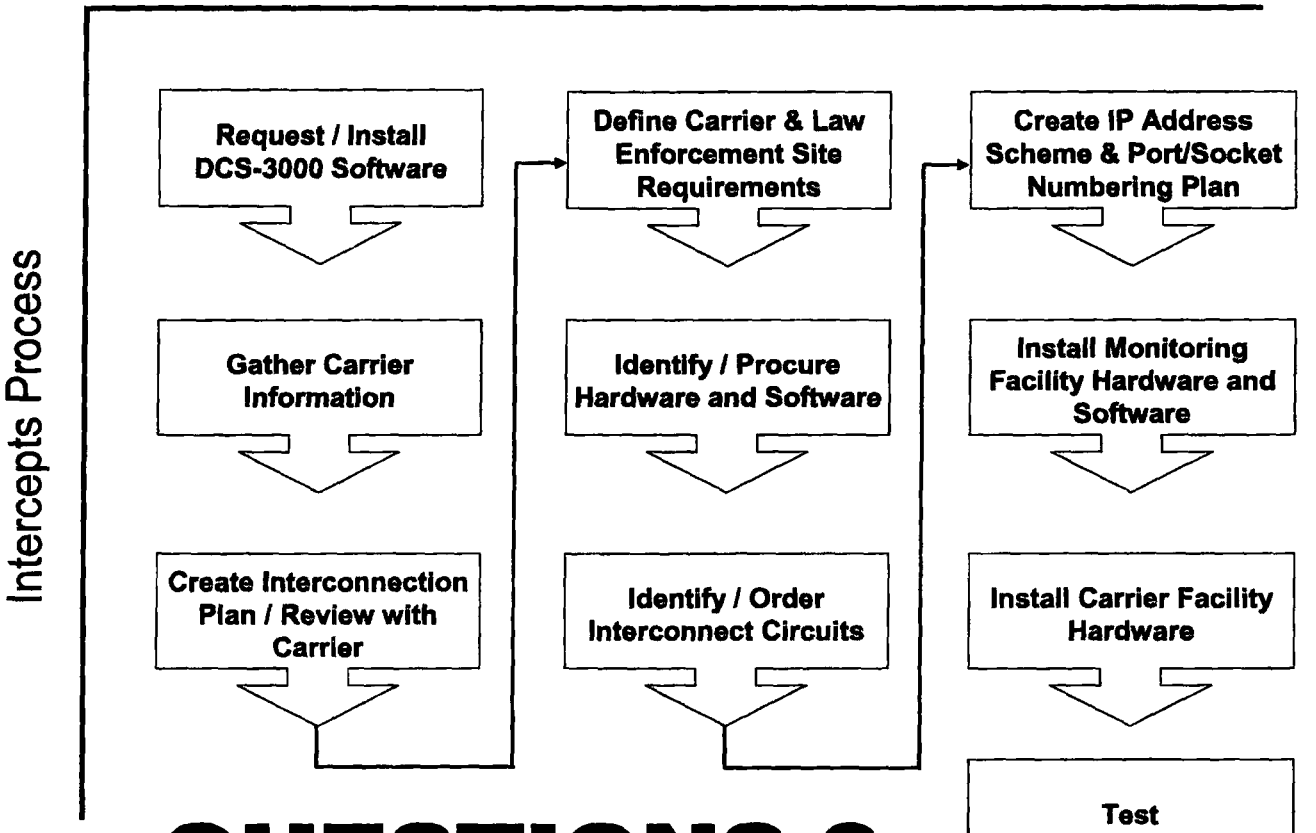
Intercepts Process



Intercepts Process



Discussion



QUESTIONS ?

DCS3000 Ver 4.2e CDNRS Record Format

Field Number	Field Size	Position	Field Contents	Field Description
1	5	1 - 5	DCSPC	Record header
2	1	7	C or R	Cleansed or raw
3	10	8 - 17	Digits	Target number
4	8	19 - 26	mm/dd/yy	Call date
5	8	28 - 35	hh:mm:ss	Start time
6	8	37 - 44	hh:mm:ss	End time
7	8	46 - 53	hh:mm:ss	Duration
8	8	55 - 62	hh:mm:ss	Ring time
9	3	64 - 66	Blanks	
10	20	68 - 87	Blanks	
11	1	89	O (outgoing) I (incoming) N (incoming unans) U (outgoing unans)	Call type
12	1	91	Blank	
13	1	93	Blank	
14	40	95 - 135		Associate number
15	3	137 - 139	Blank	
16	3	141 - 143	Blank	
17	4	145 - 148	Blank	
18	15	150 - 164	Blank	
19	25	166 - 190		Case ID (target number)
20	1	192	Y or N	Voice present
21	1	194	Blank	
22	8	196 - 203	Blank	
23	1	205	Blank	
24	20	207 - 226		Forward from call
25	20	228 - 247		Forward to call
26	20	249 - 268		Name of server
27	40	270 - 309		Warrant ID (target IMSI)
28	20	311 - 330		Cell ID

SPEAKER BIOGRAPHIES

Switch Based Intercepts Course

Engineering Research Facility
Quantico, Virginia

July 20 - 22, 2004

b6
b7C

b6
b7C

Intercepts Process

Request / Install DCS-3000 Software

- Request current copy of DCS-3000 software
- Follow authentication procedures to install software

Gather Carrier Information

- Establish primary points of contact for legal and technical issues
- Define carrier's areas of service
- Identify switching platform (vendor, model, software version)
- Identify interconnection requirements (i.e., firewall, dial-up restrictions, centralized, etc.)
- Policies and procedures
  - Roaming partner identification
  - Fee schedule
  - Future switch/software upgrade plans
  - Fail-safe measures (e.g., what data can carrier provide if interconnection disrupted?)
  - Reporting/resolving after-hour technical difficulties
  - Court orders: Acceptance by fax?
  - Court orders: Preferred wording?

Create Interconnection Plan Review with Carrier

- Define carrier configuration (centralized, decentralized, etc.)
- Identify specific interconnection locations ("Points of Presence") per switch/market

Define Carrier and Law Enforcement Site Requirements

- Equipment location (router, modem, etc.)
- Uninterruptable power source
- Location of terminating telco circuit (leased line or POTS)
- Responsibility for cable runs
- Access and security

Identify/Procure Hardware and Software

- Server/Client PC(s)
- Operating system software (Windows NT)
- Routers
- Modems
- Interconnection cables
- Title III interface card(s), if necessary

Intercepts Process

Identify/Order Interconnect Circuits

- CDC Circuits: Ringdown, POTS line at provider and CMP, ISDN
- CCC Circuits: Dial-up, leased line, may be 4 wire in middle

Create IP Address Scheme and Port/Socket Numbering Plan

- Obtain IP address from service provider
- Determine IP addresses for Ethernet and serial ports on router

Install Monitoring Facility Hardware and Software

- Monitoring equipment and software are installed in coordination with service provider

Install Carrier Facility Hardware

- Coordinate with carrier in advance (during or after regular business hours)
- Advise carrier of LE personnel who will attend)
- Have personnel available at monitoring facility for troubleshooting/testing

Test

- Connectivity
- Handset-based functional test for proper messaging

AGENDA

Interim Solutions For Telecommunications Intercepts Course

Engineering Research Facility
Quantico, Virginia

August 5 - 16, 2002

DAY ONE *Monday, August 5, 2002*

Time	Topic	Instructor
9:00 am	Welcome / Review of Course Goals & Objectives	[redacted]
9:30 am	Introduction to GSM Infrastructure	
10:30 am	BREAK	
10:45 am	Introduction to ISDN	
11:45 am	Agency / Service Provider Cooperation	
12:15 pm	LUNCH	
1:30 pm	Packet Assembler / Disassembler (PAD)	
2:30 pm	BREAK	
2:45 pm	Courier "V.Everything" Modem Configuration	
4:00 pm	Questions & Answers	

b6
b7C

DAY TWO *Tuesday, August 6, 2002*

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	[redacted]
9:15 am	Fundamentals of Cisco Router Configuration	
10:45 am	BREAK	
11:00 am	Fundamentals of Cisco Router Configuration *(cont'd)*	
12:30 pm	LUNCH	
1:30 pm	Fundamentals of Cisco Router Configuration *(cont'd)*	
3:15 pm	BREAK	
3:30 pm	Fundamentals of Cisco Router Configuration *(cont'd)*	
4:45 pm	Questions & Answers	

b6
b7C

DAY THREE Wednesday, August 7, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	Fundamentals of Cisco Router Configuration *(cont'd)*	
10:45 am	BREAK	
11:00 am	Fundamentals of Cisco Router Configuration *(cont'd)*	
12:30 pm	LUNCH	
1:30 pm	Fundamentals of Cisco Router Configuration *(cont'd)*	
3:15 pm	BREAK	
3:30 pm	Fundamentals of Cisco Router Configuration *(cont'd)*	
4:45 pm	Questions & Answers	

b6
b7C

DAY FOUR Thursday, August 8, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	Windows 2000 Operating System	
11:15 am	BREAK	
11:30 am	DCS-3000 Implementation Process	
12:30 pm	LUNCH	
1:30 pm	Advanced Carrier Solutions	
3:30 pm	Questions & Answers	

b6
b7C

DAY FIVE Friday, August 9, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	DCS-3000 Application Overview	
11:15 am	BREAK	
11:30 am	DCS-3000 Application Overview *(continued)*	
12:30 pm	LUNCH	
1:30 pm	Router Scripts and Programming Routers	
3:30 pm	BREAK	
3:45 pm	2610 Router Lab	
4:45 pm	Questions & Answers / Week 1 Evaluation & Review	

b6
b7C

DAY SIX — Monday, August 12, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	DCS-3000 Hands-On / Practical Application	
12:00 pm	LUNCH	
1:00 pm	DCS-3000 Hands-On / Practical Applications *(continued)*	
4:30 pm	Questions & Answers	

b6
b7C

DAY SEVEN — Tuesday, August 13, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	Router Debugging	
10:15 am	BREAK	
10:30 am	Basic Troubleshooting	
12:30 pm	LUNCH	
1:30 pm	DCS-3000 Hands-On / Practical Application	
4:30 pm	Questions & Answers	

b6
b7C

DAY EIGHT — Wednesday, August 14, 2002

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	DCS-3000 Hands-On / Practical Applications *(continued)*	
12:30 pm	LUNCH	
1:30 pm	Review of Log Files, CDNRS, Log Summary, etc.	
2:45 pm	BREAK	
3:00 pm	Spotlight on Nextel	
4:00 pm	Questions & Answers	

b6
b7C

DAY NINE — *Thursday, August 15, 2002*

Time	Topic	Instructor
9:00 am	Review / Goals and Objectives for Day	
9:15 am	VANguard Hands-On / Practical Applications	
12:30 pm	LUNCH	
1:30 pm	Review of Log Files, CDNRS, Log Summary, etc.	
2:45 pm	BREAK	
3:00 pm	Vendor Presentation	
4:00 pm	Questions & Answers / Week 2 Evaluation & Review	

b6
b7C

DAY TEN — *Friday, August 16, 2002*

Time	Topic	Instructor
9:00 am	Course Review	
10:00 am	Tour ERF	
12:30 pm	LUNCHEON	

b6
b7C

Federal Bureau of Investigation
Telecommunications Intercept and Collection Technology Unit

- Course Announcement -

Interim Solutions for Telecommunications Intercepts

July 2004

A. Background

Within the Federal Bureau of Investigation, the Telecommunications Intercept and Collection Technology Unit (TICTU) is the primary technical resource for the court-authorized interception of wireline and wireless communications. In late 1996, TICTU spearheaded the development of a unique telecommunications access program called "DCS-3000," a system capable of interfacing with the switching facilities of many wireless carriers that deploy new digital technologies and offer their subscribers diverse "Personal Communications Services." As the complex issues associated with the Communications Assistance for Law Enforcement Act (CALEA) are addressed, the DCS-3000 has evolved into a viable interim solution. In some cases this software has become a critical component of CALEA compliant installations.

Today, DCS-3000 systems are efficiently serving the majority of FBI field offices throughout the country. In addition, TICTU informally supports a growing number of installations for other federal, state and local law enforcement agencies. Limited unit resources and growing interest in the system have spurred the creation of a formalized training endeavor. This training effort is establishing a network of regional law enforcement specialists who are adept at all aspects of the DCS-3000 application, from installation and testing to training and trouble-shooting. Upon course completion, these Subject Matter Experts will be fully capable of maintaining their own agency installations and, on occasion, may be called upon to assist other area agencies in the implementation and maintenance of the application. This efficient "task force" approach will ensure that non-FBI agencies will continue to benefit from the research and development efforts of the Telecommunications Intercept and Collection Technology Unit.

B. Course Information

The *Interim Solutions for Telecommunications Intercepts* course is hosted at the Engineering Research Facility on the grounds of the FBI Academy in Quantico, Virginia. Classroom instruction is supplemented with lab work using bureau-provided equipment. The following is a sampling of topics included in the program of study:

- Installation and Configuration of Windows NT Operating System
- Leased and Dial-up Circuits
- Network Fundamentals / IP Addressing
- Router and Modem Configurations
- Router Debugging and Basic Troubleshooting Techniques
- DCS-3000 Software Installation, Testing and Troubleshooting
- DCS-3000 Operation and Maintenance
- Hands on Practical Exercises

C. Cost Information

The Federal Bureau of Investigation funds the two-week course of instruction, furnishes comprehensive course materials (including a course binder and CD-ROM), and provides lunchtime meals. Accommodations at the FBI Academy or local motel and additional meals are provided for out-of-town attendees. Participant host agencies are responsible for transportation expenses.

D. Participant/Agency Qualifications

The technical and sensitive nature of this training program necessitates that each participant meets several prerequisites, as explained below. To maximize training resources, applicants should expect to continue to personally conduct electronic surveillance operations for at least 12 months following training. Each applicant will be evaluated independently prior to acceptance for the course.

1. Participation is limited to practitioners whose technical responsibilities specifically include the actual implementation of court-ordered electronic surveillance activities. This course is not a planning or administrative endeavor.
2. Participant agencies must have a history of conducting such electronic surveillance operations using CALEA techniques within the past six months.
3. This is not an introductory computer course. Participants must be competent in the use of Microsoft Windows® (95, 98 or NT) operating systems.
4. Familiarity with personal computers, peripherals and interconnection cables is essential. Various aspects of the course involve configuring computer components and cables.
5. The employing agency and applicant must commit to the support of their own DCS-3000 system and agree to lend reasonable assistance in support of future installations of the DCS-3000 in their geographical area.

E. DCS-3000 Software

The DCS-3000 software is subject to distribution restrictions as established by the Department of Justice. Participants in the *Interim Solutions for Telecommunications Intercepts* course will **NOT** receive a copy of the software during the class. Instructions for requesting the software will be provided during the course.

F. Course Dates

Tuesday, August 10 through Friday, August 20, 2004.

G. Application Process

This training program is limited to ten participants per session. Additional qualified applicants will be considered for subsequent course offerings. Completed participant application forms as well as comments, questions or suggestions should be directed to:

[redacted]
Federal Bureau of Investigation
Engineering Research Facility
Building 27958-A
Quantico, VA 22135
Tel [redacted] Fax: [redacted]

b2
b6
b7C

COURSE TOPICS

Interim Solutions For Telecommunications Intercepts Course

Engineering Research Facility
Quantico, Virginia

August 10 - 20, 2004

The following topics and activities are planned at this time for discussion during the Interim Solutions course (topics are subject to change):

TECHNOLOGIES:

- GSM
- ISDN

SOFTWARE:

- Installing the DCS-3000 software
- DCS-3000 Application Overview
- Windows 2000 Operating System
- Software and Audio Card Installation
- VANGuard System

HARDWARE:

- Fundamentals of Cisco Router Configuration (2-day router course)
- Router Scripts and Programming Routers
- Router Debugging
- Basic Troubleshooting
- Courier "V.Everything" Modem Configuration
- Protocol Assembler Disassembler

MISCELLANEOUS TOPICS:

- Advanced Carrier Solutions
- DCS-3000 Implementation Process
- Review of Log Files, CDNRS, Log Summary, etc.
- Hands-on / Practical Application
- 2610 Router Lab
- Agency / Service Provider Cooperation

TOUR OF ERF LAB:

EVALUATION FORM

Interim Solutions for Telecommunicatio Intercepts Course

August 10 - 19, 2004

As a student in the third class of this type offered, your opinion is especially important in shaping this course. Please provide your comments below on the modules offered during this course and any specific recommendations for changes.

Please circle your responses to the following questions using a rating scale of 1 – 5:

1 – Strongly Disagree 3 – Agree 5 – Strongly Agree

1. Overall, the course provided a basic understanding of the CALEA paradigm and specific training using the DCS 3000 suite of applications.	1	2	3	4	5
2. The binder materials were supportive in enhancing my understanding of the sessions?	1	2	3	4	5
3. The length of the training was appropriate for the material to be presented.	1	2	3	4	5
4. The ratio of lecture to hands-on was adequate.	1	2	3	4	5
5. The subject matter in each session was covered at the level that met my needs.	1	2	3	4	5
6. Overall, this course is a valuable instructional tool.	1	2	3	4	5

7. Please comment on sessions presented that were most useful to you. Also, please comment on any sessions that you feel did not provide value:

_____

_____

_____

8. Please tell us what we should do differently for the next course (e.g., please comment on topics that should have more or less time devoted to them, thoughts on additional topics, areas that needed more or less hands-on or lecture, etc.):

_____

_____

_____

Your comments help us to improve the Interim Solutions for Telecommunications Intercepts Course.
Thank you very much for taking the time to provide your comments.

DCS-3000 Software Request Form

Federal Bureau of Investigation
Telecommunications Intercept and Collection Technology Unit

Requesting Agency Information

POC Name: _____ Title/Rank: _____

Office Telephone: _____ Office Fax: _____

Agency: _____

Shipping Address:

_____

(No P.O. boxes – Software will be sent via FedEx)

_____

_____

Justification

DCS-3000 software is provided by the FBI solely in support of cases in which a valid court authorization for electronic surveillance activities is in effect.

Request is for: _____ New Installation _____ Software Upgrade (if upgrade, current version is installed on _____ computers)

Supervisor Approval and Certification

I certify that the above information is true and correct, that the use of the DCS-3000 software will be limited to use by this agency pursuant to court authorization, and agree to properly safeguard the software against unauthorized duplication. I understand that reproduction or distribution of this software is expressly prohibited.

Title/Name of Immediate Supervisor: _____

Office Telephone: _____

Supervisor Signature: _____

---------- OFFICE USE ----------

TICTU POC: _____ Client Version: _____

Date Software Sent: _____ Multiserver Version: _____

FedEx Tracking Number: _____ VANGuard: _____

Federal Bureau of Investigation
Electronic Surveillance Technology Section
Telecommunications Intercept and Collection Technology Unit

Switch Based Intercepts Course

Switch Based Intercepts Course

b6
b7C

Electronics Engineer

Purpose

Switch Based Intercepts Course

The SBIC is an introductory course on CALEA intercept techniques and procedures. Upon completion of this course students should have a basic understanding of the CALEA Paradigm and specific training on the implementation of CALEA pen register collections utilizing the DCS 3000 suite of applications.

Background

The Switch Based Intercept Team is responsible for the development, deployment and maintenance of telephone switch-based ELSUR capabilities

DCS-3000 is the current interim solution used by the FBI

The FBI is investigating and deploying other options from outside vendors

Goals and Objectives

Switch Based Intercepts Course

Educate TTAs on:

- **Technologies utilized, FBI equipment needed, connection information for service providers, DCS-3000 application hardware, operating system, and infrastructure needed for implementation and maintenance**
- **Current issues affecting ELSUR operations**

Enable "graduates" to implement and maintain switch based intercepts in their field divisions with specific training on the DCS 3000 system

AGENDA

SWITCH BASED INTERCEPTS COURSE
July 19 – 20, 2005

Day One **Tuesday, July 19, 2005**

TIME	TOPIC	INSTRUCTOR
9:00 am	Welcome / Introduction	[redacted]
9:15 am	Goals and Objectives	
9:30 pm	Agency / Service Provider Cooperation	
9:45 am	Computer Proficiency	
10:00 am	*BREAK*	
10:15 am	Computer Proficiency *(continued)*	
11:30 am	*LUNCH*	
12:30 pm	[redacted]	
1:30 pm	Advanced Carrier Solution	
2:30 pm	*BREAK*	
2:45 pm	Courier *"v.everything"* Modem Configuration	
3:00 pm	Modem Configuration and Hands-on Application	
3:15 pm	Packet Assembler / Disassembler	
3:30 pm	Introduction to the DCS 3000 Application Suite (w/Enhancements)	
5:00 pm	Wrap-up/Questions and Answers	

b2
b6
b7C
b7E

Day Two **Wednesday, July 20, 2005**

TIME	TOPIC	INSTRUCTOR
9:00 am	Introduction to ISDN	[redacted]
10:00 am	CALEA Overview	
10:30 am	*BREAK*	
10:45 am	Event Messages and PTT Event Messages	
11:15 am	[redacted]	
11:45 pm	*LUNCH*	
12:45 pm	Hands-on Practical Application - Configuring Server and Client with Pre-programmed Router	
2:45 pm	*BREAK*	
3:00 pm	Hands-on Practical Application – Review of Log Files, CDNRS, Log Summary	
4:00 pm	Advanced DCS Topics	
4:45 pm	Course Wrap-Up / Course Evaluation /Q & A	
5:00 pm	Tour: DCS-3000 Lab	

b2
b6
b7C
b7E

Agency / Service Provider Cooperation

b6
b7C

[redacted]

Senior Consultant

SBIT Web Site

(Subset of TICTU Web Site)

ELSUR/Service Provider Cooperation

MISSION | REFERENCE | CARRIER DATA | DCS 3000 | CALEA | TRAINING | LINKS | DOWNLOADS | CONTACTS

TICTU
TELECOMMUNICATIONS INTERCEPT & COLLECTION TECHNOLOGY UNIT

Other Teams

Switch-Based Intercept Team

MISSION

Descriptions of the SBIT Vision and Mission, Who We Are, What We Do, and more...

DCS 3000

The latest software releases and User's Manual, info about DCS-3000 equipment, troubleshooting wizard, and more...

CARRIER DATA

Industry compliance guidelines, schedule of fees, points of contact, previous carrier presentations, and more...

CALEA

New info pertaining to Communications Assistance for Law Enforcement Act requirements, and more...

REFERENCE MATERIAL

Reference reports, punchlists, listings of licenses, telecom terms glossary, presentations, and more...

TRAINING

Switch Based Intercept and Interim Solutions for Telecommunication Intercept Courses, and more...

RELATED LINKS

Links to on-line government resources, telecom industry associations and news, privacy advocacy groups, and more...

DOWNLOADS

For formats provided on this site, downloadable viewers for Adobe Acrobat, Microsoft PowerPoint, Word, Excel, and more...

CONTACTS

Personnel assigned to the Switch-Based Intercept Team

Wireless Carrier Info b2 b7E

Updated 11-24-0

Updated 12-5-03

Unit Chief • Assistant

b6
b7C

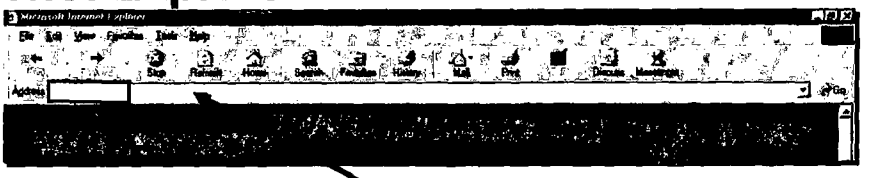
SBIT Web Site

(Subset of TICTU Web Site)

ELSUR/Service Provider Cooperation

Access through FBI Net

Internet Explorer

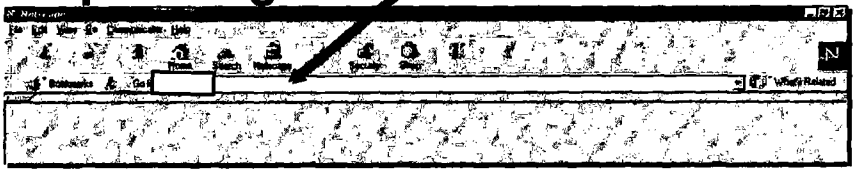


[redacted]

b2
b7E

[redacted]

Netscape Navigator



b2
b7E

SBIT Web Site

(Subset of TICTU Web Site)

ELSUR/Service Provider Cooperation

Resources

- **DCS-3000**
  - **Manual**
  - **Release Notes**
- **Reference Materials**
  - **Carrier-Specific ELSUR Material**
    - **LER Guides/POC Information**
    - **CALEA Worksheets/Fax Coversheets**
  - **CALEA Data**
  - **FCC License Information**
  - **Course Materials**
    - **SBIC**
    - **Regional Training Seminars**

DCS 3000 Applications

Collectively, the suite of DCS 3000 applications enables LEAs to intercept calls from telecommunications service providers. Each application has a specific purpose.

The DCS applications work independently of each other and in some cases a separate workstation is used for each application.

Not every DCS application is used during a surveillance operation.

Client

The Client is required for surveillance operations unless its capabilities are performed by a third-party application, such as a commercial collection platform.

- Surveillance operations are interrupted or closed from the Client.

The Client is used to:

1. enter warrants
2. collect incoming call related data (in a format suitable for use as evidence)
3. record call content.

The Client may collect data within the following guidelines:

- Supports one Title 3, Cooperative Warrant, or Push-to-Talk (PTT) collection; OR supports multiple Pen Register collections
- Connect to multiple (up to 35) Servers or MultiServers

Server

The Server receives data from the switch and routes that data to the Client.

The Server is the only application that can receive and route data for PTT calls. This application is utilized for [redacted] Call Data Channel (CDC) collection. The DCS3000 Server applicatioi has protocol and interface modes specific for the [redacted] communications. This is TICTU's primary pen-register interface for [redacted] collections. b2 b7E

The Server supports the following:

- Multiple Title 3, Cooperative Warrant, or PTT collections
- Multiple Pen Register collections
- Multiple Client connections
- Connection to one switch

VDecoder

The DCS3000 VDecoder application is a Vector Sum Excited Linear Predictor (VSELP) decode software for use with the [redacted] delivery. The DCS3000 VDecoder was the first applicationh for decoding of [redacted] udio and is an essential application for TICTU in it's current support of field operations.

b2
b7E

MultiServer

The MultiServer provides similar functionality as the Server and has the ability to connect to multiple switches

The MultiServer application is a fundamental connection application profiding for a wide array of data delivery connections. The MultiServer has incorporated into its filters several generations of proprietary switch vendor data formats including switch manufacturers such as [redacted]

Along with the filtering and processing capabilities of the MultiServer application are several protocol interfaces for accessing the required CDC or pen register information. Currently, the MultiServer supports TCP/IP connections in a client mode, FTP with login mode, serial connection with password authentication mode, timed/request initiated connection mode and GR30 (Frequency Shift Keying using caller ID specifications) mode. These modes are all utilized to perform ongoing ELSUR collections.

This application is also envisioned to be modified for future technology collections when tactically needed.

The MultiServer does *not* support PTT collections. The MultiServer supports the following:

- Multiple Title 3 and Cooperative Warrant collections
- Multiple Pen Register collections
- Multiple Client connections

VANGuard

The VANGuard buffers data fron [redacted] -compliant switches, and routes the [redacted] formatted message to the Server or MultiServer.

b2
b7E

It enables Field Offices to collect data periodically via a dial-up modem rather than a leased circuit, which reduces circuit costs.

While multiple switches connect to the VANGuard, the VANGuard connects to only one switch.

This application is also used to monitor the status of current connections to the carrier's switches. Users reset a connection if a problem is detected.

MultiVANGuard

The MultiVANGuard buffers data from multiple [redacted] switches, and sometimes is referred to as the Multiple-Switch VANGuard. b2 b7E

Like the VANGuard, the MultiVANGuard enables Field Offices to collect data periodically via a dial-up modem rather than a leased circuit, which reduces circuit costs.

The MultiVANGuard is a CDC distribution and primary server mode collections software. The MultiVANGuard has a proprietary redistribution technique based on case identification parameters. This software is currently the pathway for all CDC data collections for service providers using the [redacted] delivery system, the [redacted] delivery system , and several proprietary delivery systems being used by major wireless telecommunications carriers. b2 b7E

Also, the MultiVANGuard integrates with the DCS 5000 and DCS 6000 systems for input of CDC information for collection. These systems currently must interface through the DCS3000 MultiVANGuard. There is no vendor system available to perform the functions of the DCS3000 MultiVANGuard.

The VANGuard connects to up to 25 switches in the *Connect* mode and up to 100 switches in the *Listen* mode.

This application is also used to monitor the status of current connections to the carrier's switches. Users reset a connection if a problem is detected.

EVALUATION FORM

Switch Based Intercept Course

July 19 - 20, 2005

As a student in the third class of this type offered, your opinion is especially important in shaping this course. Please provide your comments below on the modules offered during this course and any specific recommendations for changes.

Please circle your responses to the following questions using a rating scale of 1 – 5:

1 – Strongly Disagree 3 – Agree 5 Strongly Agree

1. Overall, did the course provide a basic understanding of the CALEA paradigm and specific training using the DCS 3000 suite of applications?		1	2	3	4	5
2. How supportive were the binder materials in enhancing your understanding of the sessions?		1	2	3	4	5
3. Was the length of the training appropriate for the material to be presented?		1	2	3	4	5
4. Was the ratio of lecture to hands-on adequate?		1	2	3	4	5
5. Was the subject matter in each session covered at the level that met your needs?		1	2	3	4	5
6. Overall, this course is a valuable instructional tool.		1	2	3	4	5
7. We encourage you to visit our web-site. If you have, do you feel the TICTU website provides information relevant to you?	N/A	1	2	3	4	5

8. Please comment on sessions presented that were most useful to you. Also, please comment on any sessions that you feel did not provide value:

_____

_____

_____

9. Please tell us what we should do differently for the next course (e.g., please comment on topics that should have more or less time devoted to them, thoughts on additional topics, areas that needed more or less hands-on or lecture, etc.):

_____

_____

Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CDs

Section: 8

Federal Bureau of Investigation

b6
b7C

Reviewer: [redacted]

Commercial Payments Unit Invoice Management System (CPUIMS)	[redacted]	b6 b7C	awaiting CIO signature to be accredited	27-Feb-03	Windows 2000	WEB/DB Servers	
(S) [redacted]			IATO; 180 days to modify cert docs	27-Feb-03	Windows 2000		
Integrated Video Imaging System (IVIS)			not certified; EC drafted to Finance from Phys Sec regarding alternatives		Windows NT	WEB/DB Servers	
b1 Joint Defense Intelligence Systems Link (JDIS) operated by CRU			EC prepared to acknowledge MOA	27-Feb-03	Windows NT	WAN/LAN	MOA - YES
(S) [redacted]			awaiting CIO signature to be accredited	27-Feb-03	Windows NT	LAN	
Digital Collection system (DCS 6000); Digital Collection system (DCS 3000)			Certification; need to address comments *in their entirety*	24-Feb-03		LANS	
(S) [redacted]			2nd conditional awaiting signature	27-Feb-03	Windows 2000	LAN	ISA - YES
			not certified		Windows 2000	LAN	ISA - YES
Tactical Operations Unit Network (TOUNET)			accredited; 8/21/2002 monitoring action plan		Windows NT	WEB/DB Servers	

DATE: 05-23-2007
CLASSIFIED BY 65179DMH/KSR/MAJ
REASON: 1.4 (G)
DECLASSIFY ON: 05-23-2032

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

FBI
Assessment Team Findings
(Louisiana)

New Orleans (6/14/04-6/18/04):

- Music CD's should not be placed in computers; Memory devices should be properly labeled; Unclassified disks in classified computers; Zipdrive attached to FBINet machine; Window views not properly screened; Visitors' logs not maintained
- Computer in Technician's room not properly configured for access control (Log on)(Baton Rouge); iDEN CompanionPro terminal (NOFO) has no I&A.
- Verify PointSec requirement for CART systems; PointSec not installed on laptops
- Portable peer-less USB/Firewire drive system found- a wireless security concern; Strong wireless access point readings (Alexandria, Lafayette); TACLAN too close to the CPU (Lake Charles)
- Found numerous instances of collection systems (DCS 3000 and DCS 5000) where no workstations or servers were labeled in accordance with security documentation. It is possible that the system is not operating within the boundaries described in the CONOPS/SSP for each system
- IT positions not fully staffed. Presently short four positions, will be increased to five in the near future. Some RAs are increasing agent staff, but have not allocated additional space. Short staffing of critical technical positions increases the probability that security software and proper configuration of resources will be delayed or applied inconsistently. Overcrowding of personnel increases the probability that appropriate security procedures, such as securing sensitive information within FBI spaces, will not be observed consistently
- Need policy and procedures to track equipment brought in by JTTF members (non-FBI personnel)
- Verify C&A Status/classification of the NetSender Metrocall, FedEx, CATS, VCMO, FBIRD and HIDTA/JPSO ARMMS systems

Component Name	Major Application/General Support System Name	Unique Major Application / General Support System Identifier	Major Application / General Support System Acronym	Application or General Support System	Major Application or General Support System Description	Parent System Security Plan (SSP) Name	Scope of the SSP	Security Category G	I	A	System Development Life Cycle Status	Authorizing Official Designated Approval Authority (DAA) Name	Telephone Number	E-mail	Certification Agent Name	Telephone Number	E-mail	System Owner/Program Manager/IT Manager Name	Telephone Number	E-mail	Information System Security Manager (ISSM) Name	Telephone Number	E-mail	Information System Security Officer (ISSO) Name	Telephone Number	E-mail	User Representative Name	Telephone Number	E-mail
(S)																													
CJD	CYBERTRAKS II			System	The Language Services Section (LSS), Office of International Operations (OIO) has a requirement to procure CyberTrans II machine translation software to support agents and linguists working on major Counterterrorism investigations. The Regional Security		System	H	M	M																	
CCS	CYD Intercept Collection System		CYD IC/S	System			System																						
ITD	Data Collection Facility System		DCFS	System			System								Field Trace 4-1179														
ITD	Data Collection System 1000 (aka Carousel)		DCS 1000	System			System																						
ITD	Data Collection System 3000 (aka CALEA (Communications Assistance to Law Enforcement Act))		DCS 3000	System	DCS 3000 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		System	M	M	M																		b6 b7C
ITD	Data Collection System 6000 (aka Digital Plant)		DCS 6000	System	DCS 6000Digital Plant provides the means by which the FBI collects, stores, transcribes, and reports Electronic Surveillance (ELSUR) information in accordance with the U.S. Code Title 18. This system consolidates existing collection capabilities into		System	H	H	M																				
(S)				System	Database for external asset reporting		System																						
ITD	DCS VoIP			System			System																						
LAB	DNA LAN		DNA LAN	System			System	B	B	B																			
Bldg	Document Control System		DCS																										
LAB	Document Management System, for Racketeering Record Automation Unit		DDMS	System	The RRAU mission is to maintain records and encrypted documents, and to provide expert testimony and other forensic assistance to further criminal activity in support of Federal, State, Local, and International Law Enforcement investigations and or		System	H	H	B																				
CTD	DDS C&AM			System			System																						
	Dragflex			Application			Application																						
CD	DRUDA			System			System																						
(S)	LCF-FWS			System			System																						
CTD	ELSUR-VoIP																												
DMD	Electronic Document Entry		EDE																										
[illegible]	[illegible]		[illegible]	[illegible]			[illegible]																						
SecD	Enterprise Security Operations Center (S)		ESOC (S)	System			System	H	H	H																			
SecD	Enterprise Security Operations Center (SSU)		ESOC (SSU)	System			System																						
SecD	Enterprise Security Operations Center (TS/SCI)		ESOC (TS/SCI)	System			System																						
Bldg	Enterprise Servers (aka Mainframes-Admin and investigative)			System			System																						
LAB	Explosives Reference Tool		EXPnET	System	Explosives Unit is responsible for maintaining the FBI's explosives reference database. The Explosives Reference Tool (EXPnET) is a web-based, searchable document database that is used to assist Explosives Unit examiners in the forensic investigation		System																						
FD	FABS			System			System																						
ITD	Fairchild 7 1			System	Provide a means to remotely receive audio information for collection.		System																						
IBu	FBI HQ Secure Access Control System		FBI HQ SACS	System			System																						
	FBI HQ Server			System			System																						
IRD	FBI INTERNET		WWW.FBI.GOV	System	The mission of these systems is to deliver public affairs and other public content information to Internet users. The FBI Web Sites are the public presence of the FBI within the Internet, for both FBI HQ and the FBI Field Offices.		System																						
IRD	FBI INTERNET		WWW.FBI.GOV	System	The mission of these systems is to deliver public affairs and other public content information to Internet users. The FBI Web Sites are the public presence of the FBI within the Internet, for both FBI HQ and the FBI Field Offices.		System																						
IBu	FBI Mainframe OS & CA-TOPSECRET		Data Center	System			System																						
IRD	FBI Telephone Communications		FBI Net (aka FBI LANWAN)	WAN			WAN																						
IRD	Switch		FBI Telecomm	System			System																						
IRD	FBI Video Teleconferencing		FBI VTC	System			System	H	M	M																			
			FBI LABORATORY DIVY																										
FD	Freeport Management System		FMS	Website			Website																						
	FBISNET Topmost Guard Upgrade																												
IRD	FOIPA Document Processing System		FDPS					H	M	B																			
[illegible]	[illegible]		[illegible]	[illegible]	Applications to the Foreign Intelligence Surveillance Act (FISA) Court pass through several offices within the FBI and the Department of Justice (DOJ). An application is required [illegible]		[illegible]																						
OGC	Foreign Intelligence Surveillance Act Management System (TS/SCI)		FISA MS (TS/SCI)	System	[illegible] include document markup capabilities, collaboration tools, and a tickle system		System																						
CTD	Foreign Terrorist Tracking Task Force Bronze LAN		FTTTF Bronze	System			System																						
IRD	Foreign Visitor Information System		FVIS	System			System																						
IBu	Forensic Audio and Image Analysis Unit LAN		FAVIAU LAN (aka AVIAU LAN)	System			System																						
	FTI by ACS Data			Application			Application																						

b1
b2
b7E
b6
b7C
b6
b7C
b6
b7C

ID	System Full Name	System Short Name	SAQ Request Form	System Status	Classification	Network Domain	Exhibit 300 Reportable
1	ACS	ACS	FY07 SAQ.xls				Yes
2	Administration Mainframe Applications	AMA	FY07 SAQ.xls	Operational	Secret		Yes
3	AFIT	AFIT	FY07 SAQ.xls				Yes
4	Application Server Farm	ASF	FY07 SAQ.xls	Operational	Secret	Secret Enclave	Yes
5	Asset Validation Laptop System	AV	FY07 SAQ.xls	Operational	Secret		No
6	Automated Booking System	ABS/JABS	FY07 SAQ.xls	Operational	Unclassified/SBU		Yes
7	Background Investigative Contract Services On-line	BICS ONL	FY07 SAQ.xls	Operational	Secret		Yes
8	Bckgd Investigative Contract Service Dictaphone	BDE	FY07 SAQ.xls		Unclassified/SBU		No
9	Biometric Interoperability	BRIDG	FY07 SAQ.xls				Yes
10	Bureau Personnel Management System	BPMS	FY07 SAQ.xls	Operational	Secret		Yes
11	CALEA T-1 LAN	CALEA T-1	FY07 SAQ.xls	Operational	Unclassified		No
12	Campus WAN	CWAN	FY07 SAQ.xls	Operational	Unclassified/SBU		No
13	CJIS Wide Area Network	CJIS WAN	FY07 SAQ.xls	Operational	Unclassified	Other	Yes
14	Combined DNA Indexing System	CODIS	FY07 SAQ.xls	Operational	Unclassified		Yes
15	Commercial Payments Unit Invoice Management System	CPUIMS	FY07 SAQ.xls	Operational	Secret	Secret Enclave	Yes
16	Compass IT	Compass IT	FY07 SAQ.xls		Secret		Yes
17	Computer Analysis Response Team Area Network	CARTSAN	FY07 SAQ.xls	Operational	Secret		No
18	Computer Analysis Response Team Storage Area Networ	CART SAN	FY07 SAQ.xls	Operational	Secret		Yes
19	Consolidated Asset Tracking System Controlled Interface	CATSCI	FY07 SAQ.xls	Operational	Secret		Yes
20	COOP Duplicate VNS Trusted Guard	VNS TG	FY07 SAQ.xls		Unclassified/SBU		Yes
21	Cryptoanalysis Initiative Computer Net	CI-NET	FY07 SAQ.xls	Operational	Secret		No
22	Cryptographic & Electronic Analysis Unit SCIF CPU	CEAU SCIF CPUs	FY07 SAQ.xls	Operational	TS/SCI		No
23	CyberTrans	CyberTrans	FY07 SAQ.xls	Operational	Secret	Secret Enclave	No
24	CyberTrans/CyberTrans II	CyberTrans II	FY07 SAQ.xls	Operational	Secret	Secret Enclave	No
25	Data Collection Network	DCN	FY07 SAQ.xls	Operational	TS/SCI		No
26	Data Collection System 3000	DCS 3000	FY07 SAQ.xls	Operational	Unclassified		Yes
27	Data Collection System 5000	DCS 5000; Redwolf	FY07 SAQ.xls	Operational	Secret		Yes
28	Data Collection System 6000	DCS 6000, Digital Storm	FY07 SAQ.xls	Operational	Unclassified		Yes
29	Data Extraction and Extension Project OMB-300	DEEP	FY07 SAQ.xls	Operational	Secret	Secret Enclave	Yes
30	Data Loading and Analysis	DaLAS	FY07 SAQ.xls				Yes
31	Digital Collection System Network	DCSNET	FY07 SAQ.xls	Operational	Unclassified		Yes
32	Digital Document Management System	DDMS	FY07 SAQ.xls	Operational	Secret		No
33	DirectorNet	DirectorNet	FY07 SAQ.xls	Operational	Secret		No
34	Disposition Records Improvement	Disposition Records	FY07 SAQ.xls				Yes
35	Document Capture System OMB-300	DOCLAB; DCS	FY07 SAQ.xls	Operational	Secret		Yes
36	Domain Mapping Initiative Proof of Concept	ARC	FY07 SAQ.xls	Operational	Secret		Yes
37	[redacted]		FY07 SAQ.xls	Operational	TS/SCI		No
38	EFTIS	EFTIS	FY07 SAQ.xls				Yes
39	Electronic Key Management System SECRET	EKMS	FY07 SAQ.xls	Operational	Secret		No
40	Electronic Key Mgmt Sys (TS)	EKMS - TS	FY07 SAQ.xls	Operational	TS/SCI		No
41	Emergency Alert Messaging System	ePOP	FY07 SAQ.xls	Development	Secret		Yes
42	Enhanced IAFIS Repository	Enhanced IAFIS	FY07 SAQ.xls				Yes
43	Enterprise Sec Ops Center Phase 2	ESOC P2	FY07 SAQ.xls	Operational	TS/SCI		Yes
44	Enterprise Security Ops Center Phase III	ESOC P3	FY07 SAQ.xls	Operational	Secret		Yes
45	Enterprise Servers	Enterprise Servers	FY07 SAQ.xls	Operational	Secret		Yes

(S)

b1
b2
b7E

DATE: 05-24-2007
CLASSIFIED BY 65179DMH/KSR/MAJ
REASON: 1.4 (G)
DECLASSIFY ON: 05-24-2032

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FISMA Reportable	FISA	PIA	PIA Date	C&A Required	C&A Expiration Date
No					
Yes	No	No		Yes	07/26/2009
No					
Yes	Yes	No		Yes	6/14/2008
Yes	No	No		No	
No	No	No		No	
No	No	No		Yes	10/23/2005
Yes	No	No		Yes	12/7/2007
No					
Yes	No	No		Yes	12/7/2007
Yes	No	No		Yes	4/16/2007
Yes	No	No		No	
Yes	No	No		Yes	2/9/2005
Yes	No	No		Yes	3/8/2005
No	No	No		Yes	9/29/2007
No	No	No		Yes	9/6/2008
Yes	No	No		Yes	
Yes					
No	Yes	No		Yes	
No					
Yes	No	No		Yes	
Yes	No	No		Yes	
Yes	No	No		Yes	12/14/2006
Yes	No	No		Yes	6/30/2007
Yes	No	No		No	
No	No	No		Yes	5/29/2008
No	No	No		Yes	11/25/2008
No	No	No		Yes	5/30/2006
Yes	No	No		Yes	2/7/2008
No					
No	No	No		Yes	
Yes	No	No		Yes	
Yes	No	No		Yes	
No					
Yes	No	No		Yes	8/10/2008
No					
Yes	No	No		No	
No					
Yes	No	No		Yes	5/17/2008
Yes	No	No		No	
No					
No					
Yes	No	No		No	
Yes					
Yes	No	No		Yes	11/30/2007

~~SECRET~~

ID for June submission	Investment Name (Program Name)	Includes these Systems[1]	NIST FIPS 199 Risk Impact Level	Date C&A completed	Date security controls tested	Date contingency plan tested	Comments
FY08-027	Digital Collection	1) DCS 3000 2) DCS 5000 3) DCS 6000	1) Med 2) High 3) Med Differ than what it says in business case	1) 6/1/06 2) 2/3/06 3) 6/2/06	1) 5/3/06 2) 11/05 3) 5/26/06	1) 5/31/06 2) 5/22/06 3) 9/1/05 (?)	8/21: DCS 6000 is not on the FY2006 FISMA list. 9/1 Updated version did not incorporate my comments.
FY08-028	Systems Engineering Services	Unknown – says SES/SOA prototype but I think it should include the T&D environment instead.					
FY08-029	IT Infrastructure Rebuild	Information Portal	TBD	N/A	N/A	N/A	Planned operational date is 6/15/2007.
FY08-030	Enterprise Telephony	PTSS (?)	High	7/21/05	5/18/05	5/31/06	Business case listed various switches in the planning table that it calls operational – it wasn't clear to me how what is in this business case relates to PTSS. I provided comments to the author and requested clarification. Dates I provided relate to PTSS.
FY08-031	CIO Enterprise Support	N/A					

~~SECRET~~

FBI Security Division (SecD) Information Assurance Section (IAS)
Certification Unit (CU) and Information Technology Security Unit (ITSU)
Certification and Accreditation (C&A) Efforts

Certification and Accreditation Status

Status	TS/SCI	TS	S	SBU	UND	*Totals*
Accredited	5	1	26	20		52
Accredited w/ Action Plan	4		4	2		10
IATO	6	1	17	9		33
Certified			4	1		5
Undergoing Certification	7		32	31	2	72
Registered	5		13	22	3	43
Totals	**27**	**2**	**96**	**85**	**5**	**215**

System	*Classification*	*CUST*	*Approval*	*Granted*	*Req. IOC*	*Effort Type*	*Cert Team*	*Effort Status*
Administrative Mainframe Applications (Admin MF Apps)	Secret	IRD	Operate	12-Jul-01	11-Jul-04	Reaccred Original		Undergoing Certification Accredited w/ Action Plan
Annual Field Office Report (AFOR)	Secret	CTD	Operate	09-Apr-02	09-Apr-05	Original		Accredited w/ Action Plan
Anti-Drug Network (ADNET)	Secret	CCD	Operate	15-Dec-01	14-Dec-04	Reaccred Original		IATO Accredited
Application Server Farm (ASF) (aka Mini-Server Farm)	Secret	IRD				Original		Undergoing Certification
ARACHNET	Secret					Original		Undergoing Certification
Asset Validation Laptop	Secret	CD				Original		Undergoing Certification
Automated Booking System (ABS)	Sensitive But Unclassified	CJIS	Operate	27-May-03	26-May-06	Original		Accredited
Automatic Call Distribution (ACD)	Sensitive But Unclassified	IRD	Interim	15-Apr-03	14-Jun-03	Original		IATO
Background Investigative Contract Services (BICS On-Line)	Secret	ASD	Operate	24-Oct-02	23-Oct-05	Original		Accredited
Bomb Scene Response and Reporting Kit (BSRRK) (aka COBRA)	Sensitive But Unclassified	LAB				Original		Undergoing Certification
Building Management System (BMS)	Sensitive But Unclassified	CJIS				Original		Undergoing Certification
Bureau Personnel Management System (BPMS)	Sensitive But Unclassified	IRD	Operate	01-Jul-00	30-Jun-03	Reaccred Original		Undergoing Certification Accredited

b6
b7C

DATE: 05-29-2007
CLASSIFIED BY 65179dmh/ksr/maj
REASON: 1.4 (G)
DECLASSIFY ON: 05-29-2032

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

System	Classification	CUST Approval		Granted	Req. IOC	Effort Type	Cert Team	Effort Status
Computer Assisted Facility Management System (CAFMS)	Sensitive But Unclassified	ASD				Original	CU-HAL	Undergoing Certification
Consolidation McIntosh LAN (MAC LAN)	Sensitive But Unclassified	CJIS				Original		Undergoing Certification
Continuum (aka AMAPP)	Undetermined	CIRG				Original		Registered
Controlled Interface 100 (CI-100) (aka Spidernet, OWF)	Secret	SecD	Operate	20-Feb-04	19-Feb-07	Original		Accredited
Cornerstone	Secret	CD				Original		Undergoing Certification
Correspondence Management System (CMS) (aka TRIM)	Secret	RMD	Interim	30-Jul-03	30-Jan-04	Original		Certified
Counterterrorism Reporting Syst on Suspicious Surveillance (CROSS) (aka HSRS)	Sensitive But Unclassified	CTD	Interim	06-Feb-04	05-Aug-04	Original		ATO
Criminal Intelligence Information System (CIIS)	Secret	CID				Original		Registered
Critical Reach (aka TRAK)	Sensitive But Unclassified	LV				Original		Registered
Cryptoanalysis Initiative Computer Net (CI NET)	Secret	ITD	Operate	20-Aug-01	19-Aug-04	Original		Accredited
Cryptographic & Electronic Analysis Unit's SCI Facility Computers (CEAU SCIF CPUs) (aka SCIF Net)	Top Secret SCI	ITD	Operate	07-May-03	07-May-06	Original		Accredited
CV - Lost Child Alert Technology Resource (LOCATOR) (aka NCMEC)	Sensitive But Unclassified	CV				Original		Registered
Cyber Sweep	Sensitive But Unclassified	WF	Operate			Original		Undergoing Certification
(S) CYBERTRANS II	Secret	OIO	Operate	14-Jun-04	13-Jun-07	Original		Accredited
[redacted]	Top Secret SCI	ITD	Operate	27-Feb-03	27-Feb-06	Original		Accredited
Data Collection System 3000 (DCS 3000) (aka CALEA (Communications Assistance to Law Enforcement Act))	Sensitive But Unclassified	ITD	Operate	29-May-03	28-May-06	Original		Accredited
Data Collection System 5000 (DCS 5000)	Secret	ITD				Original		Undergoing Certification
Data Collection System 6000 (DCS 6000) (aka Digital Storm)	Sensitive But Unclassified	ITD	Operate	30-May-03	29-May-06	Original		Accredited w/ Action Plan
(S) [redacted]		CD				Original		Undergoing Certification
[redacted]	Secret	ITD				Original		Registered
Demon	Undetermined	ITD				Original		Registered

b6
b7C
b1
b2
b7E

(S)

For Official Use Only

Operation Mayday

System	*C&&A*	*Classification*	*Status*
(U) Data Collection System 3000 (DCS 3000) (aka CALEA (Communications Assistance to Law	ITSU	Secret	In Review for Accreditation
(U) Data Collection System 6000 (DCS 6000) (aka Digital Storm)	ITSU	Sensitive But Unclassified	In Review for Accreditation
(U) FAVIAU LAN (aka AUDIO LAN)	ITSU	Secret	In Review for Accreditation
(U) Integrated Video Imaging System (IVIS)	ITSU	Secret	In Review for Accreditation
(U) LAZY DOG	ITSU	Sensitive But Unclassified	In Review for Accreditation
(U) LIGHTPLANE	ITSU	Top Secret	In Review for Accreditation
(U) OPDC LAN	ITSU	Sensitive But Unclassified	In Review for Accreditation
(U) OPDC Stand-alone	ITSU	Secret	In Review for Accreditation
(U) SCIF Net	CU	Top Secret SCI	In Review for Accreditation
(U) SDIS	ITSU	Top Secret SCI	In Review for Accreditation
(U) Service Center (aka Peregrine Systems Service	ITSU	Secret	In Review for Accreditation
(U) SIOC Public Access LAN (PAL) to include TIPS db	ITSU	Sensitive But Unclassified	In Review for Accreditation
(U) TTAPNET	ITSU	Top Secret SCI	In Review for Accreditation
(S) [redacted]	CU	Secret	In Review for Accreditation
(U) Uniform Crime Reporting (UCR)	ITSU	Undetermined	In Review for Accreditation
(U) Automated Booking System (ABS)	**ITSU**	**Sensitive But Unclassified**	**In Progress**
(U) CART LAN (aka CMAL)	**ITSU**	**Sensitive But Unclassified**	**In Progress**
(U) CJIS ISS	**ITSU**	**Secret**	**In Progress**
(U) CODIS	**ITSU**	**Secret**	**In Progress**
(U) CTD MAC Presentation System	CU	Top Secret SCI	In Progress
(U) FBI HQ SACs	**ITSU**	**Secret**	**In Progress**
(U) FBI INTERNET (WWW.FBI.GOV)	**ITSU**	**Sensitive But Unclassified**	**In Progress**
(U) FBI TELEPHONE COMMUNICATIONS	**ITSU**	**Sensitive But Unclassified**	**In Progress**
(U) Field Office Integrated Security System (FO ISS)	ITSU	Secret	In Progress
(U) FOIPA Document Processing System (FDPS)	**CU**	**Secret**	**In Progress**
(U) Greendoor Internet Network (aka Newington Internet)	ITSU	Sensitive But Unclassified	In Progress
(U) Key Asset Database	CU	Secret	In Progress
(U) Law Enforcement Online (LEO)	ITSU	Sensitive But Unclassified	In Progress
(U) NIPC Watch LAN	ITSU	Secret	In Progress
(U) Personnel Security Unit Systems (PSUS)	**CU**	**Secret**	**In Progress**
(U) Training Campus WAN (includes Virtual Academy)	**ITSU**	**Sensitive But Unclassified**	**In Progress**
(U) Washington Metro Security Systems (WMSS)	**ITSU**	**Secret**	**In Progress**

b1
b2
b7E

**** Systems in Bold/Blue will exercise DOJ assistance for C&A activities as coordinated with UCs [redacted]**
POCs for DOJ Team are FBI - [redacted] and DOJ - [redacted]
DOJ Team are available in Room 1B948 and via Groupwise Email.
DOJ Team members are:

[redacted]

b6
b7C

DATE: 05-31-2007
CLASSIFIED BY 65179dmh/ksr/maj
REASON: 1.4 (G)
DECLASSIFY ON: 05-31-2032

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Recommended Action: Prioritize hiring of key technical personnel. Engage appropriate resources to allocate space for personnel, as staffing increases.

Problem: Guidance needed regarding labeling of periphery devices. Some devices remain unlabelled.

Problem: Zipdrive attached to FBINet machine.

Recommended Action: Complete Trilogy User training. Remind users not to attach unauthorized devices to network. Remind users not to install unauthorized software. Treat future instances as security violations and report through appropriate channels with increasingly severe penalties for repeat violations.

Problem: iDEN CompanionPro terminal (NOFO) has no I&A.

Recommended Action: Install required identification and authentication (username/password) meeting DOJ 2640.2E requirements prior to accessing application.

Problem: Outdated or no disk encryption on laptop computers.

Recommended Action: Install PointSec on all machines unless excepted. Provide written justification to SecD for consideration of any exceptions.

Problem: Baton Rouge RA, CART laptop has no disk encryption.

Problem: Found numerous instances of collection systems (DCS 3000 and DCS 5000) where no workstations or servers were labeled in accordance with security documentation. It is possible that the system is not operating within the boundaries described in the CONOPS/SSP for each system.

Recommended Action: The Security Division should verify that each system is operating within security parameters described in the documentation. The DCS 3000 and DCS 5000 should document discrepancies and initiate recommended corrective action or deactivate systems.

Systems Found

JTTF Unclass
CART Unclass
CATS Secret
NCIC terminals
MetroCall/ Net Sender
SAMNET
iDEN CompanionPro
Innocent Images
Rapid Start
FedEx tracking system
DCS3000 (Title III) Unclass
DCS5000 [redacted] Unclass
JABS

b2
b7E

Trilogy Problem: NetOps backup problems. Documented in P34569, P30966 dated May 6, 2004. ITs in correct Admin Group but do not have permissions.

Recommended Action: Follow up on PRs; respond to [redacted]

Trilogy Problem: Logon screen defaults to username of last user when logging on to system. Found at Lafayette RA on various machines.

Recommended Action: Generate PR. Survey all machines by property number to establish which machines to apply PR.

b6
b7C

Trilogy Problem: Cannot print Trilogy Rules of Behavior.

Recommended Action: Follow up and respond to [redacted].

Trilogy Problem: Workstation intermittently "hangs" when logging off. User profile problem?

Trilogy Concern: Cannot open all attachments at the same time.

Trilogy Concern: User must check box to verify, when attempting to save to local drive.

Trilogy Concern: Why Active Directory structured with single domain @ HQ and not multiple domains. [redacted]

Recommended Action: Follow up and respond.

Combined Report

Operational FBI Information Systems

Certification and Accreditation Status - Legacy Systems

Status	*Top Secret/SCI*	*Top Secret*	*Secret*	*SBU*	*Totals*
Accredited	6	1	20	15	42
Accredited w/ Action Plan	1		2	5	8
IATO	2		1	3	6
In Review for Accreditation			4		4
In Progress			4	7	11
Delayed			1	2	3
Totals	9	1	32	32	74

Certification and Accreditation Status - New Systems

Status	*Top Secret/SCI*	*Top Secret*	*Secret*	*SBU*	*UND*	*Totals*
Accredited	1		7	2		10
Accredited w/ Action Plan			1			1
IATO	4		7	3		14
In Progress	2		1	1		4
Research			1			1
Totals	7		17	6		30

System	*Classification*	*Status*	*C&&A*	*Accred. Date*	*Comments*
Automated Booking System (ABS)	Sensitive But Unclassified	Accredited	ITSU	27-May-03	
Automatic Call Distribution (ACD)	Sensitive But Unclassified	IATO	CU	15-Apr-03	
Bureau Personnel Management System	Sensitive But Unclassified	Accredited	ITSU	01-Jul-00	
Centra Server	Sensitive But Unclassified	Accredited	ITSU	01-Nov-02	
CHEMNET	Sensitive But Unclassified	In Progress	ITSU		
CODIS	Sensitive But Unclassified	In Progress	ITSU		
Computer Analysis Response Team Family of Systems (CART FOS) (aka CART LAN)	Sensitive But Unclassified	Accredited	ITSU	30-Jul-03	
Data Collection System 3000 (DCS 3000) (aka CALEA (Communications Assistance to Law Enforcement Act))	Sensitive But Unclassified	Accredited	ITSU	29-May-03	
Data Collection System 6000 (DCS 6000) (aka Digital Storm)	Sensitive But Unclassified	Accredited w/ Action Plan	ITSU	30-May-03	
DNA LAN	Sensitive But Unclassified	In Progress	ITSU		
FAVIAU LAN (aka AUDIO LAN)	Sensitive But Unclassified	Accredited w/ Action Plan	ITSU	03-Jul-03	
Greendoor Internet Network (aka Newington Internet)	Sensitive But Unclassified	Delayed	ITSU		

Tier Level	Definition	Systems accredited during FY 2006
Tier 2	**Confidentiality Goals**: BASIC, MEDIUM or HIGH **System Security Concept**: PL1 or PL2* Dedicated & System High Mode * *Connectivity is authorized only if an approved Controlled Interface is used to adjudicate the security policies between connected systems. **Integrity and Availability Goals**: MEDIUM or HIGH for Dedicated Mode or PL1 BASIC or MEDIUM for System High Mode or PL2 **Examples**: More complicated/integrated systems Systems with higher operational criticality or sensitivity System that impacts another directorate or office	BSR Safeguard ABS TS/SCI Enclave [redacted] WTO-PTSS CWAN DCS-6000 RDS BICS-Online RDPS [redacted] RMS SPYB-PTSS FOISS ICDMI DCS 3000 DCS 5000 IISNET VICAP [redacted] AMA
Tier 3	**Confidentiality Goals**: BASIC, MEDIUM or HIGH **System Security Concept**: PL2 or PL3* System High & Compartmented Mode* *Connectivity is authorized only if an approved Controlled Interface is used to adjudicate the security policies between connected systems. **Integrity and Availability Goals**: HIGH for System High Mode or PL2 BASIC, MEDIUM, or HIGH for Compartmented Mode or PL3 **Examples:** Systems that provide the day-to-day support of critical FBI missions. System that impacts multiple directorates or offices FBI global wide-area networks. One-Way Transfer Controlled Interface	ESOC TOUNET FAMS-C Secret Enclave RCI IICMS DirectorNet FDF-A NICS-E/Check CJIS WAN TSC OWT-CI IAFIS IMA WEBTA POC ESAN PACMS PED ESAN
Tier 4	**Confidentiality Goals**: HIGH **System Security Concept**: PL4 or PL5 Multi-Level Mode **Integrity and Availability Goals**: BASIC, MEDIUM, or HIGH **Examples**: Multi-Level or PL4/PL5 systems Multi-Level Control Interfaces (Guards) - Requires two-way communication between systems at different classifications.	CATS-CI

(S)

(S)

(S)

b1
b2
b7E

From: [redacted]
To:
Date: Thu, Mar 21, 2002 9:03 AM
Subject: Re: meetings

Thanks [redacted]

>>> [redacted] 03/21 8:38 AM >>>
[redacted] This was only a preliminary meeting to discuss how we are going to approach documenting the certification of the DCS 3000 system as that Program Office have Booz, Allen and Hamilton on-board to develop the documentation for their system. When we meet with them regarding policy and procedures we will definitely want the accreditation and testing memebers to be a part of the discussion [redacted] b6 b7C

>>> [redacted] 03/20 1:20 PM >>>
[redacted]
I know you probably forgot to contact me about Quantico, but in the future would you please contact me when you remember? It was just as well I stayed here and did some reading, but I could have caught up with your group in Quantico.
[redacted]

Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CDs

Section: 10

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 62
Page 44 ~ Duplicate To Division CD's section 1
Page 45 ~ Duplicate To Division CD's section 1
Page 46 ~ Duplicate To Division CD's section 1
Page 47 ~ Duplicate To Division CD's section 1
Page 48 ~ Duplicate To Division CD's section 1
Page 49 ~ Duplicate To Division CD's section 1
Page 50 ~ Duplicate To Division CD's section 1
Page 51 ~ Duplicate To Division CD's section 1
Page 52 ~ Duplicate To Division CD's section 1
Page 53 ~ Duplicate To Division CD's section 1
Page 54 ~ Duplicate To Division CD's section 1
Page 55 ~ Duplicate To Division CD's section 1
Page 56 ~ Duplicate To Division CD's section 1
Page 57 ~ Duplicate To Division CD's section 1
Page 58 ~ Duplicate To Division CD's section 1
Page 59 ~ Duplicate To Division CD's section 1
Page 60 ~ Duplicate To Division CD's section 1
Page 61 ~ Duplicate To Division CD's section 1
Page 62 ~ Duplicate To Division CD's section 1
Page 63 ~ Duplicate To Division CD's section 1
Page 64 ~ Duplicate To Division CD's section 1
Page 65 ~ Duplicate To Division CD's section 1
Page 66 ~ Duplicate To Division CD's section 1
Page 67 ~ Duplicate To Division CD's section 1
Page 68 ~ Duplicate To Division CD's section 1
Page 69 ~ Duplicate To Division CD's section 1
Page 70 ~ Duplicate To Division CD's section 1
Page 71 ~ Duplicate To Division CD's section 1
Page 72 ~ Duplicate To Division CD's section 1
Page 73 ~ Duplicate To Division CD's section 1
Page 74 ~ Duplicate To Division CD's section 1
Page 75 ~ Duplicate To Division CD's section 1
Page 76 ~ Duplicate To Division CD's section 1
Page 77 ~ Duplicate To Division CD's section 1
Page 78 ~ Duplicate To Division CD's section 1
Page 79 ~ Duplicate To Division CD's section 1
Page 80 ~ Duplicate To Division CD's section 1
Page 81 ~ Duplicate To Division CD's section 1
Page 82 ~ Duplicate To Division CD's section 1
Page 83 ~ Duplicate To Division CD's section 1
Page 84 ~ Duplicate To Division CD's section 1
Page 85 ~ Duplicate To Division CD's section 1
Page 86 ~ Duplicate To Division CD's section 1
Page 87 ~ Duplicate To Division CD's section 1

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

Page 88 ~ Duplicate To Division CD's section 1
Page 89 ~ Duplicate To Division CD's section 1
Page 90 ~ Duplicate To Division CD's section 1
Page 91 ~ Duplicate To Division CD's section 1
Page 92 ~ Duplicate To Division CD's section 1
Page 93 ~ Duplicate To Division CD's section 1
Page 94 ~ Duplicate To Division CD's section 1
Page 95 ~ Duplicate To Division CD's section 1
Page 96 ~ Duplicate To Division CD's section 1
Page 97 ~ Duplicate To Division CD's section 1
Page 98 ~ Duplicate To Division CD's section 1
Page 99 ~ Duplicate To Division CD's section 1
Page 100 ~ Duplicate To Division CD's section 1
Page 101 ~ Duplicate To Division CD's section 1
Page 102 ~ Duplicate To Division CD's section 1
Page 103 ~ Duplicate To Division CD's section 1
Page 104 ~ Duplicate To Division CD's section 1
Page 105 ~ Duplicate To Division CD's section 1

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

[redacted] (RMD) (FBI)

From: [redacted] (SecD)(CON)
Sent: Wednesday, May 31, 2006 3:03 PM
To: [redacted] (SecD) (FBI)
Cc: [redacted] (SecD) (CON)
Subject: DCS 3000 EC

b6
b7C

UNCLASSIFIED
NON-RECORD

DCS-3000 CERT EC
05302006.wpd

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

b2
b6
b7C

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-21-2007 BY 65179 DMH/TAM/KSR/cb #1056287

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: Immediate Date: 05/31/2006

To: Security Attn: [redacted]

From: Security
Information Assurance Section/Certification/SPY-B F-601
Contact: [redacted] (202) [redacted]

Approved By: [redacted]

Drafted By: [redacted] cjp

b6
b7C

Case ID #: 319U-HQ-1487677-SECD- (Pending)

Title: IT SYSTEMS SECURITY RISK ANALYSES
INFORMATION ASSURANCE SECTION (IAS)
CERTIFICATION UNIT (CU)
DIGITAL COLLECTION SYSTEM-3000 (DCS-3000)
SECURITY TEST REPORT

Synopsis: Certification Unit's validation findings conducted on the DCS-3000 Risk Management Matrix RMM), dated 26 May, 2006.

Reference: (1) 319U-HQ-1487677-SECD-275

Administrative: Additional References:
(2) DCS-3000 System Security Plan (SSP) (U//FOUO), dated 28 April, 2006
(3) DCS 3000 Risk Management Matrix (RMM) (U//FOUO), dated 5 November, 2002
(4) DCS 3000 Certification Executive Summary Report (U//FOUO), dated 26 May, 2006

Details: In order to facilitate the decision to re-accredit the DCS-3000 system, the Accreditation Unit (AU) requested that Certification Unit validate the eight (8) findings documented in Reference (3) as being properly mitigated or closed.

In accordance with the FBI Certification and Accreditation Handbook, the DCS-3000 system has been assessed as a Tier Level 2 with levels of concern (LOC) of Medium for Confidentiality, Integrity, and Availability. The DCS-3000 system is a Sensitive But Unclassified (SBU) system operating in the System High Mode of Operation Reference (1).

Enterprise Security Operations Center (ESOC) Testing personnel assisted Certification Unit by performing validation of the

eight (8) findings identified in the RMM Reference (3). The results of the validation testing are in the Certification Executive Summary Report Reference (4). Validation results concluded that three (3) of the six(6) were corrected. One (1) vulnerability was found to be a false finding. The last finding, lack of the Intrusion Detection System (IDS), has not been corrected or mitigated.

Certification testing on the DCS-3000 system was performed during an initial C&A effort four years ago. Due to the age of the previous Certification assessment, as well as proposed changes to the current architecture, the Certifier recommends that full Certification testing be performed on the DCS-3000 system.

LEAD(s):

Set Lead 1: (Action)

SECURITY

AT WASHINGTON, DC

Attn: Accreditation Unit. Coordinate the accreditation decision for the DCS-3000 System.

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

Attn: ISSM, [redacted] for your information.

CC: [redacted]

b6
b7C

♦

[redacted]RMD) (FBI)

From: [redacted](SecD) (FBI)
Sent: Friday, June 02, 2006 12:40 PM
To: [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](SecD)(FBI); [redacted](SecD)(CON)
Cc: [redacted](SecD) (FBI); [redacted](SecD) (CON); [redacted](SecD) (FBI); [redacted](SecD)(CON)
Subject: DCS3000 ATO EC

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

If you have any additional questions please contact [redacted]

DCS-3000 ATO EC 06012006.wpd

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-21-2007 BY 65179 DMH/TAM/KSR/cb

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 06/01/2006

To: Operational Technology Attn: [redacted]

Security Attn: [redacted]

b6
b7C

From: Security
Information Assurance/Accreditation/SPY-B F-501
Contact: [redacted], 202-[redacted]

Approved By: [redacted]

Drafted By: [redacted]:mlm

Case ID #: 319U-HQ-A1487677-SECD Serial#305

Title: IT SYSTEM SECURITY RISK ANALYSES
INFORMATION ASSURANCE SECTION (IAS)
ACCREDITATION UNIT (AU)
ACCREDITATION DECISION: GRANT APPROVAL
TO OPERATE (ATO) WITH CONDITIONS FOR DIGITAL
COLLECTION SYSTEM 3000 (DCS-3000)

Synopsis: Grant an ATO with conditions for DCS-3000 for a period of 3 years.

Reference: 319U-HQ-A1487677-SECD Serial 300

Administrative: References:
(1) System Security Plan (SSP), dated 04/28/2006
(2) Security Test Report, date 05/26/2006
(3) Risk Management Matrix (RMM), dated 06/01/2006
(4) Risk Management Plan (RMP), dated 06/01/2006
(5) Plan of Action and Milestone (POA&M), dated 06/01/2006

Details: The Security Division's Accreditation Unit (AU) conducted a review of the Certification Documents, reference above, for the DCS-3000 in accordance with the requirements set forth by Bureau, Departmental, National policy, and the FBI Certification and Accreditation Handbook. The Designated Accrediting Authority (DAA) grants an ATO with conditions for a period of 3 years starting on 06/01/2006 and expiring on 06/01/2009.

The accreditation boundary of the DCS-3000 includes the DCS-3000 application suite that consists of five (5) component applications residing on one or more workstations. The components of the DCS suite used to support a particular requirement depend upon the type of surveillance to be conducted, the switch providing the data, the telecommunications service provider, and availability of equipment at the field office.

The DCS-3000 is operating at the Sensitive But Unclassified level in the System High mode of operation. The system has been designated as Tier 2 system that operates at a Medium level of concern (LoC) for Confidentiality, Integrity, and Availability.

The following summarizes the risks associated with Management, Operational, and Technical controls of DCS-3000. Additional details are contained in Risk Management Plan (RMP), Reference (4):

Management Controls: No open Management control vulnerabilities were identified within the previous RMM; however, during the security review it was discovered that the system had not undergone a full security assessment in over 4 years. Therefore, it is recommended the system undergo a full security assessment within 180 days.

Operational Controls: Although the previous RMM identified no remaining vulnerabilities within this control, it was identified during the security review that system security documentation contained discrepancies that needed to be addressed. These discrepancies have been documented within the DCS-3000 SSP Errata Sheet.

Technical Controls: Only two vulnerabilities remain within this area. Vulnerability #5 has been deemed accepted risk. Vulnerability #7 is being researched by the system owner and has been addressed within the POA&M, Reference (5).

In conclusion, based on the findings of the security review and the defined migration plan, in addition to the existing mitigations as identified in POAM, the Accreditation Unit recommends an Approval To Operate for 3 years with the following conditions:

1. A full security assessment be completed within 180 days to ensure appropriate security controls have been implemented that address changes in the architecture that have occurred.

2. All vulnerabilities be successfully resolved or mitigated within the 180 day period.

Failure to meet these conditions will result invalidation of this ATO and require full re-certification and re-accreditation of the DCS-3000 system.

Any major change(s) to DCS-3000 shall be brought to the attention of the Information System Security Manager (ISSM).

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

Coordinate with ISSM to resolve outstanding POA&M actions and coordinate full security assessment of the DCS-3000. In addition, if major changes are made to the system characteristics or accreditation boundary during the ATO period, please notify the Information System Security Manager (ISSM).

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

Coordinate with System Owner to resolve outstanding POA&M actions and set up full system security assessment. Report status of POA&M to Accreditation Unit.

CC: [redacted]

b6
b7C

♦♦

[redacted] (RMD) (FBI)

From: [redacted] (SecD) (FBI)
Sent: Thursday, June 01, 2006 12:22 PM
To: [redacted] (SecD) (FBI); [redacted] (SecD)(FBI)
Cc: [redacted] (SecD)(CON); [redacted] (SecD) (CON); [redacted] (SecD) (FBI); [redacted] (SecD)(CON)
Subject: DCS3000 Cert EC

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

If you have any additional questions please contact [redacted]

DCS-3000 CERT EC
05302006.wpd

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-21-2007 BY 65179 DMH/TAM/KSR/cb

[redacted], (RMD) (FBI)

From: [redacted] (SecD) (FBI)
Sent: Thursday, May 04, 2006 3:12 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (SecD)(FBI); [redacted] (SecD)(CON)
Cc: [redacted] (SecD) (FBI); [redacted] (SecD) (CON); [redacted] (OTD) (FBI); [redacted] (SecD)(CON); [redacted] (SecD) (FBI)
Subject: DCS-3000

b6
b7C

UNCLASSIFIED
NON-RECORD

Attached is the uploaded documentation for the DCS-3000. For additional information contact eithe[redacted]

Thank you.
[redacted]

DCS-3000 Tier EC 05012006.wpd

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-21-2007 BY 65179 DMH/TAM/KSR/cb

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 05/2/2006

To: Operational Technology Attn: [redacted]

Security Attn:

b6
b7C

From: Security
Information Assurance/Accreditation/SPY-B F-501
Contact: [redacted] 202-[redacted]

Approved By: [redacted]

Drafted By: [redacted]:mlm

Case ID #: 319U-HQ-1487677-SECD-275

Title: IT SYSTEMS SECURITY RISK ANALYSES
INFORMATION ASSURANCE SECTION (IAS)
ACCREDITATION UNIT (AU)
DIGITAL COLLECTION SYSTEM 3000 (DCS-3000)
ACCREDITATION DECISION:
SECURITY CHARACTERISTIC AND TIER LEVEL
DESIGNATION FOR DCS-3000

Synopsis: Designate the DCS-3000 Tier Level, Mode of Operation, determine the Confidentiality, Integrity, Availability Levels, Boundary description, and name the key Certification and Accreditation Team Members.

Administrative: DCS-3000 Accreditation Boundary Diagram, dated 05/1/2006.

Details: As a result of correspondence and meetings with the Accreditation Representative, Information System Security Manager, Information System Security Officer, Certification Representative, the DCS-3000 Program Manager and System Administrator, the following security characteristics and Tier Level have been determined and agreed upon.

The Levels of Concern (LoC) are Medium for Confidentiality, Medium for Integrity, and Medium for Availability. DCS-3000 is a Sensitive but Unclassified (SBU) system operating in the System High Mode of Operation. The DCS-3000 has been assessed as a Tier Level 2 in accordance with the FBI Certification and Accreditation Handbook.

The DCS-3000 application suite was developed to assist Law Enforcement Agencies (LEA) with collecting and processing data for court-ordered Electronic Surveillance (ELSUR) operations. The DCS-3000 collects [redacted] ata from the Telecommunications Service Provider (TSP) and stores it at the LEA site. b2 b7E

The DCS-3000 application suite consists of five (5) component applications residing on one or more workstations. The components of the DCS suite used to support a particular requirement depend upon the type of surveillance to be conducted, the switch providing the data, the telecommunications service provider, and availability of equipment at the field office.

The Certification and Accreditation Team Members are:

System Owner: [redacted]
Information System Security Officer:
System Administrator:
Information System Security Manager:
Certification Representative:
Accreditation Representative:

[redacted] b6 b7C

LEAD(s):

Set Lead 1: (Info)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

Notify the ISSM if there are any changes to DCS-3000 that could impact its designation of the Tier Level, Levels of Concern, Mode of Operation, and accreditation boundary.

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

For information only.

CC:

b6
b7C

♦♦

[redacted] RMD) (FBI)

From: [redacted] (SecD)(CON)
Sent: Wednesday, May 31, 2006 3:48 PM
To: [redacted] SecD) (FBI)
Cc: [redacted] (SecD) (CON)
Subject: FW: DCS 3000 EC (CORRECTED COPY)

UNCLASSIFIED
NON-RECORD

DCS-3000 CERT EC 05302006.wpd

[redacted] here is the corrected copy of the ec

b2
b6
b7C

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phon[redacted]
Fax[redacted]

-----Original Message-----
From: [redacted] D)(CON)
Sent: Wednesday, May 31, 2006 3:03 PM
To: [redacted] ecD) (FBI)
Cc: [redacted] ecD) (CON)
Subject: DCS 3000 EC

UNCLASSIFIED
NON-RECORD

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone:[redacted]
Fax:[redacted]

UNCLASSIFIED

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-22-2007 BY 65179 DHM/TAM/KSR/cb

[redacted] (RMD) (FBI)

From: [redacted] SecD)(CON)
Sent: Friday, May 26, 2006 1:29 PM
To: [redacted] ecD) (CON)
Subject: FW: Dcs 3000 RMM

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

[redacted] see matrix end of matrix..chart.
[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax [redacted]

-----Original Message-----
From: [redacted] (SecD) (CON)
Sent: Friday, May 26, 2006 1:15 PM
To: [redacted] ecD)(CON)
Subject: RE: Dcs 3000 RMM

b6
b7C

UNCLASSIFIED
NON-RECORD

The dcs3000 rmm -

DCS3000 RMM_052606.doc

UNCLASSIFIED

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-22-2007 BY 65179 DMH/TAM/KSR/cb

DCS3000

Systems Security Plan
Appendix C
Risk Management Matrix (RMM)

November5, 2002

Version 1.0 – November 5, 2002

b6
b7C

Prepared For:
Ms. [redacted]
Chief, Legacy System Certification Unit (LSCU)
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Room 1302
Washington, DC 20530

Prepared By:
LSCU Green Team
FBIHQ

1. INTRODUCTION

1.1. System Description

DCS3000 is a computer-based intelligence collection systems used by FBI personnel to

[redacted]

b2
b7E

- Facilitates the review and examination of the information
- Dramatically increases the efficiency of trial preparations
- [redacted]
- Exponentially increases the utility and value of computer-based intercepts

b2
b7E

The DCS3000 system is deployed in central monitoring plants (CMP) located in FBI field offices and at the FBI Engineering Research Facility (ERF). Access to the field office buildings and the ERF is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).

FBI professionals, who have been well screened, cleared, and trained for the operations they perform, operate and use the system in a physically secure, climate-controlled environment. The system is easy to use, and personnel duties are clearly defined and appear to be commonly understood so stress levels for system users, regardless of their positions, are fairly low, especially in light of the types of work they do.

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

- An initial pre-certification test (i.e., vulnerability assessment) of the DCS3000 system during the period August 22-23, 2002.
- Personal interviews with cognizant DCS3000 program management and technical personnel.
- Analysis of FBI field-office personnel surveys

2. RISK ASSESSMENT RESULTS

This section provides detailed DCS3000 risk assessment results that were derived from the initial pre-certification testing. Vulnerabilities and threats have been paired by severity of risk after all applicable existing safeguards relative to them have been taken into account. It is important to note that multiple vulnerability/threat pairs may be discussed by vulnerability if similar safeguards can mitigate the pairs. Test results were generally favorable and justified no further testing of this system for the purposes of this C&A effort.

For each vulnerability/threat pair, the following information is included in narrative form:

- The vulnerability/threat pair number (e.g., 1, *2*, etc.)
- Vulnerability/threat pair description (in *italics*)
- Description of the probable impact on the pair and analysis of the impact (also in *italics*)
- Planned or recommended controls or alternative options for reducing risks

2.1. Risk Assessment

2.1.1. High Risk Vulnerability/Threat Pairs

The following are high-risk vulnerability/threat pairs that are drawn from the RMM table. There are seven operational aspects of this collection system that appear to be at high risk but easily mitigated. Overarching mitigating factors for these risks include the DCS3000 working environment at each operating location (i.e., FBI field office, resident agency (RA) office, etc.) that is tightly controlled and protected by multi-layered physical security, and the personnel within it, who participate in electronic surveillance (ELSUR) operations and who must undergo a very thorough and comprehensive screening process in order to be granted an FBI Top Secret clearance before being authorized to perform their tasks.

The following are the associated high-risk vulnerability pairs drawn from the RMM table below:

1. There is no anti-viral software loaded on the DCS3000 machines. If malicious code, viruses, and/or executables are introduced, there will be potential for risk to the system or compromise of data, thereby compromising evidence contained therein.

Planned or Recommended Remedial Action:

- Install FBI approved anti-virus software on all servers and workstations.
- System administrators ensure all virus signatures are updated weekly or as needed.

b2
b7E

Planned or Recommended Remedial Action:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

b2
b7E

3. Successive failed logon attempt lockout is not enabled. Without a lockout policy, an unauthorized user would have infinite attempts to gain access to the system.

Planned or Recommended Remedial Action:

- Account lockout duration
- Account lockout threshold (i.e. 3 attempts)
- Unlock procedures

5. Workstations associated with the system do not enforce adequate user permissions. Improperly configured machines do not adhere to the least privilege principle. This practice could potentially give a user access and rights not warranted for by their position.

Planned or Recommended Remedial Action:

Recommend the implementation of workstation permissions to give least privilege access.

6. The improper account (i.e. guest or administrator) configurations do not provide the facility for adequate auditing.

Planned or Recommended Remedial Action:

Recommend deleting the guest accounts and renaming the administrator accounts.

7. The system lacks an intrusion detection capability. This functionality provides warning of an unauthorized access or user to the system.

Planned or Recommended Remedial Action:

Recommend implementing an intrusion detection scheme.

8. The Telnet login process is accomplished in the "clear". This practice compromises the user ID and password information.

Planned or Recommended Remedial Action:

Recommend a secure Telnet implementation.

2.1.2. Medium Risk Vulnerability/Threat Pairs

The following medium-risk vulnerability/threat pair is drawn from RMM table below.

4. Auditing was found to be inadequate. Tracking users actions will allow records to be kept for accountability purposes. These records can be used for investigations and to track system or network problems for troubleshooting purposes.

Planned or Recommended Remedial Action:

Recommend implementing workstation and server auditing and log dumps on a daily basis to reduce impact on resources.

Overall, recommend Senior FBI management personnel should take a very active role in support of a comprehensive FBI INFOSEC program. As part of this program, a comprehensive FBI information security (INFOSEC) training program should be developed and implemented throughout the FBI. Also, unit-level, job-specific INFOSEC training should be strongly encouraged or mandated.

RISK MANAGEMENT MATRIX FOR DCS 3000			
[illegible]	[illegible]	[illegible]	[illegible]
1. No anti-virus software found. VL = High	HIGH	Methods to be used to limit the risk: - Install FBI approved anti-virus software on all servers and workstations. - System administrators ensure all virus signatures are updated weekly or as needed. RR = Low	Verified McAfee 4.5.1 installed with Virus updated 05/05/2006
2. Insufficient password management controls VL = High	HIGH	Recommend enforcing mandated password policies. As a minimum: - An eight-character password composed of at least three of the following, English uppercase, English lower case, numeric, special characters. - Prevent the use of the previous six passwords. - Expire an initial use password at the time of its first use in a manner that requires the password owner to supply a new password. - Prevent the display of a clear text password. RR = Low	Verified Passwords required to be 8 characters, complex etc.
3. Insufficient account lockout policy VL = High	HIGH	Recommend instituting an account lockout policy by implementing, at a minimum: - Account lockout duration - Account lockout threshold (i.e. 3 attempts) - Unlock procedures RR = Low	Verified Accounts lock out after three attempts and must be reset by admin.
4. Inadequate audit logging. VL = Medium	MEDIUM	Recommend implementing workstation and server auditing and log dumps on a daily basis to reduce impact on resources. RR= Low	Routers syslog and systems event viewer is set to record all events.

Vulnerability (V)	Risks to Assets R = (T x V) x S	Mitigating or Recommended Countermeasures Residual Risk (RR)	
5. Improper workstation permissions. VL = High	HIGH	Recommend the implementation of workstation permissions to give least privilege access. RR= Low	N/A Software required to run with admin privledges. See SSP.
6. Improper guest/administrator account configuration. VL = High	HIGH	Recommend deleting the guest accounts and renaming the administrator accounts. RR = Low	Verified Guest account is disabled and the Administrator account is renamed.
7. Lack of Intrusion Detection Systems (IDS) VL = High	HIGH	Recommend implementing an intrusion detection scheme. RR = Low	No IDS is installed.
8. Telnet login is not encrypted VL = High	HIGH	Recommend a secure Telnet implementation. RR = Low	Verified Telnet is not being used.

[redacted] (RMD) (FBI)

From: [redacted] (SecD)(CON)
Sent: Thursday, May 25, 2006 3:42 PM
To: [redacted] SecD)(CON)
Cc: [redacted] (OTD) (FBI) [redacted] SecD) (FBI) [redacted] SecD) (CON)
Subject: FW: Dcs 3000 TEST at Quantico

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

[redacted] from ESOC test group will test DCS 3000 tomorrow for us at quantico.

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

-----Original Message-----
From: [redacted] (SecD)(CON)
Sent: Thursday, May 25, 2006 3:35 PM
To: [redacted] ecD) (CON)
Subject: FW: Dcs 3000 RMM

UNCLASSIFIED
NON-RECORD

Here is thanks a lot.

b2
b6
b7C

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

-----Original Message-----
From: [redacted] (SecD)(CON)
Sent: Thursday, May 25, 2006 11:41 AM
To: [redacted] ecD)(CON)
Subject: Dcs 3000 RMM

UNCLASSIFIED
NON-RECORD

DCS3000
RMM_060203.doc

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] SecD)(CON)
Sent: Thursday, June 01, 2006 1:00 PM
To: [redacted] (SecD) (CON)
Subject: FW: DCS 3000

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
b7C

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

-----Original Message-----
From: [redacted] (SecD) (FBI)
Sent: Thursday, June 01, 2006 11:29 AM
To: [redacted] SecD) (FBI); [redacted] (SecD)(FBI); [redacted] (SecD)(CON); [redacted] (SecD) (FBI)
Subject: DCS 3000

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

The attached EC has been uploaded. For additional information, please contatct [redacted] [redacted]

b6
b7C

DCS-3000 CERT EC
05302006.wpd

[redacted]
Information System Security Representative (ISSR)
Western Region
SPYB F-601 [redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] SecD)(CON)
Sent: Tuesday, May 23, 2006 10:46 AM
To: [redacted] SecD) (CON)
Subject: FW: DCS-3000 SSP

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fa[redacted]

-----Original Message-----
From: [redacted] TD) (FBI)
Sent: Tuesday, May 23, 2006 10:05 AM
To: [redacted] ecD)(CON)
Cc: [redacted] SecD)(CON)
Subject: DCS-3000 SSP

UNCLASSIFIED
NON-RECORD

b6
b7C

Here is the final draft of the SSP for the DCS 3000.

[redacted]

DCS3000 System Security Plan 2...

UNCLASSIFIED

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-22-2007 BY 65179 DMH/TAM/KSR/cb

[redacted] (RMD) (FBI)

From: [redacted] SecD)(CON)
Sent: Thursday, June 01, 2006 2:44 PM
To: [redacted] (SecD) (CON)
Subject: LOOK... Quick!!! (DCS-3000 POA&M)

UNCLASSIFIED
NON-RECORD

b6
b7C

DCF3000 POAM.doc

It was QUICK!!! Let me know if ya need something more!!!

[redacted]
Information System Security Manager (ISSM)
Quantico Complex
CISM, CISSP, ISS, PSEC, MCSE
[redacted]
... lead, follow, or get out of the way. Thomas Paine

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-23-2007 BY 65179 DMH/TAM/KSR/cb

Data Collection System 3000 (DCS-3000)

Plan Of Actions & Milestones (POA&M)

June 1, 2006

Version 1.0

b6
b7C

Prepared by:

Quantico ISSM

Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington DC 20530

1. INTRODUCTION

1.1. System Description

DCS-3000 is a computer-based intelligence collection systems used by FBI personnel to

[redacted] b2 b7E

- Facilitates the review and examination of the information
- Dramatically increases the efficiency of trial preparations

[redacted] b2 b7E

- Exponentially increases the utility and value of computer-based intercepts

The DCS-3000 system is deployed in central monitoring plants (CMP) located in FBI field offices and at the FBI Engineering Research Facility (ERF). Access to the field office buildings and the ERF is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).

FBI professionals, who have been well screened, cleared, and trained for the operations they perform, operate and use the system in a physically secure, climate-controlled environment. The system is easy to use, and personnel duties are clearly defined and appear to be commonly understood so stress levels for system users, regardless of their positions, are fairly low, especially in light of the types of work they do.

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

- A security assessment of the DCS-3000 system was conducted during the period May 2, 2006 to verify closure of open vulnerabilities.
- Personal interviews with DCS-3000 program management and technical personnel.

2. RISK ASSESSMENT RESULTS

This section provides detailed DCS-3000 risk assessment results that were derived from the initial pre-certification testing. Vulnerabilities and threats have been paired by severity of risk after all applicable existing safeguards relative to them have been taken into account. It is important to note that multiple vulnerability/threat pairs may be discussed by vulnerability if similar safeguards can mitigate the pairs. Test results were generally favorable and justified no further testing of this system for the purposes of this C&A effort.

For each vulnerability/threat pair, the following information is included in narrative form:

- The vulnerability/threat pair number (e.g., 1, *2*, etc.)
- Vulnerability/threat pair description (in *italics*)
- Description of the probable impact on the pair and analysis of the impact (also in *italics*)
- Planned or recommended controls or alternative options for reducing risks

2.1. Risk Assessment

2.1.1. High Risk Vulnerability/Threat Pairs

The following are the remaining high-risk vulnerability/threat pairs that are drawn from the initial RMM table. There are seven operational aspects of this collection system that appear to be at high risk. Overarching mitigating factors for these risks include the DCS-3000 working environment at each operating location (i.e., FBI field office, resident agency (RA) office, etc.) that is tightly controlled and protected by multi-layered physical security, and the personnel within it, who participate in electronic surveillance (ELSUR) operations and must undergo a thorough and comprehensive screening process in order to be granted an FBI Top Secret clearance before being authorized to perform their tasks.

The following are the validated closed and remaining associated high-risk vulnerability pairs below:

1. There is no anti-viral software loaded on the DCS-3000 machines. If malicious code, viruses, and/or executables are introduced, there will be potential for risk to the system or compromise of data, thereby compromising evidence contained therein.

Current Status:

- Verified Closed: McAfee 4.5.1 installed with Virus updated 05/05/2006

b2
b7E

Current Status:

- Verified Closed: Passwords require eight characters, complex etc.

3. Successive failed logon attempt lockout is not enabled. Without a lockout policy, an unauthorized user would have infinite attempts to gain access to the system.

Current Status:

- Verified Closed: Accounts lock out after three attempts and must be reset by admin.

5. Workstations associated with the system do not enforce adequate user permissions. Improperly configured machines do not adhere to the least privilege principle. This practice could potentially give a user access and rights not warranted for by their position.

Current Status:

- Remains Open: Software required to run with admin privileges. See SSP.

Planned or Recommended Remedial Action:

- Recommend the implementation of workstation permissions to give least privilege access.

6. The improper account (i.e. guest or administrator) configurations do not provide the facility for adequate auditing.

Current Status:

- Verified Closed: Guest account is disabled and the Administrator account is renamed.

7. The system lacks an intrusion detection capability. This functionality provides warning of an unauthorized access or user to the system.

Current Status:

- Remains Open: No IDS is installed.

Planned or Recommended Remedial Action:

Recommend implementing an intrusion detection scheme.

8. The Telnet login process is accomplished in the "clear". This practice compromises the user ID and password information.

Current Status:

- Verified Closed: Telnet is not being used.

2.1.2. Medium Risk Vulnerability/Threat Pairs

The following medium-risk vulnerability/threat pair is drawn from RMM table below.

4. Auditing was found to be inadequate. Tracking users' actions will allow records to be kept for accountability purposes. These records can be used for investigations and to track system or network problems for troubleshooting purposes.

Current Status:

- Verified Closed: Routers syslog and systems event viewer is set to record all events.

This assessment was conducted to verify remaining vulnerabilities; however, due to age of the original test report and proposed changes to the current architecture a full system security assessment is required. These requirements are being added to the DCS-3000 Plan of Action and Milestones (POA&M) as risk management items that require the appropriate attention for resolution.

RISK MANAGEMENT MATRIX FOR DCS-3000

Risk Analysis				Risk Management
Vulnerability (V)	Threat (T) to Asset	Significance (S) of Occurrence	Risks to Assets (R) = (T x V) x S	Mitigating or Recommended Countermeasures Residual Risk (RR)
1. No anti-virus software found. VL = High	Introduction of malicious code, viruses and or executables to DCS-3000 systems/networks without detection TL = High	If malicious code, viruses, and/or executables are introduced, there will be potential for risk to system or compromise of data SL = High	HIGH	Closed
2. Insufficient password management controls VL = High	The system does not enforce adequate password policies, thereby allowing unauthorized access. TL = High	[redacted] SL = High	HIGH	Closed b2 b7E
3. Insufficient account lockout policy VL = High	The system does not enforce an account lockout policy. TL = High	Without a lockout policy, an unauthorized user would have infinite attempts to gain access to the system. SL = High	HIGH	Closed
4. Inadequate audit logging. VL = Medium	Low gain from exploitation TL = Medium	Tracking users actions will allow records to be kept for accountability purposes. These records can be used for investigations and to track system or network problems for troubleshooting purposes. SL = High	MEDIUM	Closed

RISK MANAGEMENT MATRIX FOR DCS-3000

Risk Analysis				Risk Management
Vulnerability (V)	Threat (T) to Asset	Significance (S) of Occurrence	Risk to Asset R = G x V x S	Mitigating or Recommended Countermeasure Residual Risk (RR)
5. Improper workstation permissions. VL = High	Workstations associated with the system do not enforce adequate user permissions. TL = Medium	Improperly configured machines do not adhere to the least privilege principle. SL = High	HIGH	Recommend the implementation of workstation permissions to give least privilege access. RR= Low
6. Improper guest/administrator account configuration. VL = High	Workstations allow guest accounts and have not deleted or renamed the administrator accounts. TL = High	The improper configurations do not provide the facility for adequate auditing. SL = High	HIGH	Closed
7. Lack of Intrusion Detection Systems (IDS) VL = High	System lacks intrusion detection capability. TL = High	Lack of intrusion detection provides vulnerabilities to the system. SL = High	HIGH	Recommend implementing an intrusion detection scheme. RR = Low
8. Telnet login is not encrypted VL = High	Telnet capability is unprotected. TL = High	Telnet login is accomplished in the clear. SL = High	HIGH	Closed

Concerns

(U) There are several areas of the total DCS-3000 program that require additional correction/improvement. Because the final engineering of the system is not completed, and the former certification testing was accomplished approximately four years ago, a full system test is required once the system architecture has achieved stasis. In addition, the DCS-3000 SSP requires the corrections noted by the Certification Unit (CU) to include updated system drawings, expanded concept of operations, and the corrections listed on the provided errata sheet.

(U) The documentation will be completed as soon as possible, and the certification testing must be accomplished within 180 days of this POA&M approval.

(U) The existing open RMM identified items also require resolution.

Conclusion

(U) The DCS-3000 has very few existing vulnerabilities, and is an SBU system. The addition of the [redacted] (server) connection does not appear to introduce an increase in risk significant enough to not recommend that it be allowed. This added capability will significantly improve the mission capability, while introducing a very low risk connection. b2 b7E

(U) I believe this system is operated and maintained at an acceptable level of risk. I, therefore, recommend that the DCS-3000 be given a three year ATO with the caveats listed in paragraph 2 & 3 of the "Concerns" above.

(U) I also recommend that the failure to meet these conditions should invalidate the ATO and require full recertification and re-accreditation of the DCS-3000 system.

[redacted] (RMD) (FBI)

From: [redacted] (SecD) (FBI)
Sent: Thursday, June 01, 2006 12:36 PM
To: [redacted] (SecD) (FBI); [redacted] (SecD) (FBI) [redacted] (SecD)(FBI)
Cc: [redacted] (SecD)(CON); [redacted] (SecD) (CON); [redacted] (SecD)(CON)
Subject: RE: DCS3000 Cert EC

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Hello to All:

[redacted] was able to upload the Cert EC earlier (Ref. EC 319U-HQ-1487677-SECD-300)

[redacted]

-----Original Message-----
From: [redacted] SecD) (FBI)
Sent: Thursday, June 01, 2006 12:22 PM
To: [redacted] (SecD) (FBI); [redacted] SecD)(FBI)
Cc: [redacted] SecD)(CON) [redacted] SecD) (CON) [redacted] (SecD) (FBI [redacted] (SecD)(CON)
Subject: DCS3000 Cert EC

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

If you have any additional questions please contact [redacted]

<< File: DCS-3000 CERT EC 05302006.wpd >>

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-23-2007 BY 65179 DMH/TAM/KSR/cb

[redacted] (RMD) (FBI)

From: [redacted] SecD)(CON)
Sent: Thursday, June 01, 2006 1:44 PM
To: [redacted] SecD) (CON)
Subject: RE: DCS-3000 POA&M

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

.. Just got back from a (hostile) CSO meet'n, but I'll try!!

b6
b7C

[redacted]
Information System Security Manager (ISSM)
Quantico Complex
CISM, CISSP, ISS, PSEC, MCSE
[redacted]
..."lead, follow, or get out of the way." Thomas Paine

-----Original Message-----
From: [redacted] (SecD) (CON)
Sent: Thursday, June 01, 2006 1:42 PM
To: [redacted] SecD)(CON)
Subject: DCS-3000 POA&M

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Will you be able to complete before 3pm?

MM

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-23-2007 BY 65179 DMH/TAM/KSR/cb

[redacted] (RMD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Wednesday, April 26, 2006 3:06 PM
To: [redacted] SecD) (CON)
Subject: RE: DCS-3000 Tier EC and Boundary Document

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

The figure in the Word document is accurate.

[redacted]

-----Original Message-----
From: [redacted] (SecD) (CON)
Sent: Wednesday, April 26, 2006 8:09 AM
To: [redacted] (SecD)(CON); [redacted] (OTD) (FBI)
Cc: [redacted] SecD)(CON); [redacted] (SecD) (FBI)
Subject: DCS-3000 Tier EC and Boundary Document
Importance: High

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

All,

I have completed an updated architectural drawing. Please take a look and let me know if it is accurate. I want to get the Tier EC out this week and get things moving on this system.

Regards, << File: DCS-3000 Accreditation Boundary Diagram.vsd >> << File: DCS3000 Accreditation Boundary.doc >>

[redacted]

[redacted] CISSP
SecD/IAS/AU
[redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-23-2007 BY 65179 DMH/TAM/KSR/cb

[redacted] RMD) (FBI)

From: [redacted] (SecD)(CON)
Sent: Tuesday, May 23, 2006 10:55 AM
To: [redacted] (SecD) (CON)
Subject: SRTM FOR DCS 3000

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

DCS 3000.xls

[redacted]
Information Assurance Analyst
SecD/IAS/CU (Certification Unit)
"Certification lead, Team #2"
Phone: [redacted]
Fax: [redacted]

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-23-2007 BY 65179 DMH/TAM/KSR/cb