U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

ESQ. MARCIA HOFMANN
ELECTRONIC FRONTIER FOUNDATION
SUITE 650
1875 CONNECTICUT AVENUE, NORTHWEST
WASHINGTON, DC 20009

July 2, 2007

Subject: SYSTEM DCS-3000 and Red Hook

FOIPA No. 1056287- 000 and FOIPA No. 1056307-1

Dear Ms. Hofmann:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552

□(b)(1)

☒(b)(2)

□(b)(3)________________________

____

____

____

□(b)(4)

□(b)(5)

☒(b)(6)

□(b)(7)(A)

□(b)(7)(B)

☒(b)(7)(C)

□(b)(7)(D)

☒(b)(7)(E)

□(b)(7)(F)

□(b)(8)

□(b)(9)

Section 552a

□(d)(5)

□(j)(2)

□(k)(1)

□(k)(2)

□(k)(3)

□(k)(4)

□(k)(5)

□(k)(6)

□(k)(7)

811 **page(s)** were reviewed and 711 **page(s)** are being released.

□ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

□ referred to the OGA for review and direct response to you.

□ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information and Privacy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001 within sixty days from the date of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

□ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

Please be advised that this is the second interim release as ordered by the court on May 7, 2007 for documents concerning electronic surveillance systems known as DCS-3000 and Red Hook.

A decision has not been made concerning your request for a waiver of fees. We will be corresponding with you concerning that request in the near future. In the interim, we are providing you with the enclosed documents. Pursuant to Title 28, Code of Federal Regulations, Section 16.11, there is a fee of ten cents per page for duplication. No fees are assessed for the first 100 pages. If it is determined that you do not qualify for a fee waiver, duplication fees will be assessed accordingly.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CDs

Section: 1

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

Federal Bureau of Investigation

FBI System Security Plan (SSP)

Federal Bureau of Investigation (FBI)
SYSTEM SECURITY PLAN (SSP)

DCS 3000
System Security Plan

Date: 28 April 2006

Version: 2.0

SSP Template Rev. 3.0

System Owner: Operational Technology Division

Table of Contents

List of Figures

List of Tables

Attachments

RECORD OF CHANGES AND REVIEW

Number	Date	Description	Entered By

DCS 3000 System Security Plan

INTRODUCTION

The DCS 3000 is an Electronic Surveillance (ELSUR) collection system that supports Criminal Law Enforcement (CLE) as well as Foreign Intelligence Surveillance Act (FISA) Pen Register investigations. The Operational Technology Division (OTD), Electronic Surveillance Technology Section (ESTS), Telecommunications Intercept and Collection Technology Unit (TICTU) developed and deployed the DCS 3000 system in Central Monitoring Plants (CMPs) in various FBI offices. This SSP documents the security policies and procedures for the DCS 3000 system. In addition, this plan delineates responsibilities and expected behavior of all individuals who access the system. This plan establishes the approved operational baseline and configuration and is the basis for the type certification and accreditation of the DCS 3000, regardless of the physical location of systems within the FBI. This document has been prepared in accordance with guidance provided by the FBI Certification and Accreditation (C&A) Handbook Version 2.1, June 1, 2005.

1. INFORMATION SYSTEM GENERAL INFORMATION

1.1 Security Administration

1.1.1 System Information

Information System Name	**DCS 3000**
Information System Number (if applicable)	**66F-HQ-C1333650-DCS3000**
Date of Plan	**28 April 2006**
Revision/Version	**Version 2.0. Reevaluation of system resulting from expiration of accreditation expiring May 26, 2006**
TSABI Number (if applicable)	**Not Applicable (N/A)**
Web Location for documentation (if applicable)	**FBINET/TICTU**
Status (New System or Modification to an Existing System)?	**Operational System**
Project ID (if applicable)	**N/A**
Deployment Installation Date	**Currently Deployed**
Security Test & Evaluation Date	**28 May 2003**
Required Operational Date	**Currently Operational**

1.1.2 Key System Points of Contact

System Owner	Name	[redacted]
	Organization	TICTU
	Address	[redacted]
	Phone: Commercial	[redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[redacted]
Accreditor	Name	
	Organization	
	Address	
	Phone: Commercial	
	Phone: Secure	
	Pager	

b6
b7C

	Email Address	
Certifier	Name	
	Organization	
	Address	
	Phone: Commercial	
	Phone: Secure	
	Pager	
	Email Address	
ISSM	Name	[redacted]
	Organization	Operational Technology Division
	Address	[redacted]
	Phone: Commercial	[redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[redacted]
ISSO	Name	[redacted]
	Organization	TICTU
	Address	[redacted]
	Phone: Commercial	[redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[redacted]
ISSO Alternate	Name	[redacted]
	Organization	TICTU
	Address	[redacted]
	Phone: Commercial	[redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[redacted]
System Administrator	Name	[redacted]
	Organization	TICTU
	Address	[redacted]
	Phone: Commercial	[redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[redacted]

b6
b7C

1.1.3 Security Organization

The information system security program for the DCS 3000 is managed and implemented by the TICTU of the ESTS of the FBI's OTD [redacted] and the ISSO for the DCS 3000 program. Attachment A describes the organizational structure for the management of this system. b6 b7C

1.2 Mission

1.2.1 Purpose and Scope

The DCS 3000 is an ELSUR collection system that supports Pen Register criminal investigations as well as FISA investigations. The system was developed to assist Law Enforcement Agencies (LEAs) with collecting and processing court-ordered ELSUR operations.

To conduct court-ordered ELSUR operations, the FBI dials into switches, which are devices used by Telecommunications Service Providers (TSPs) to route telephone calls to their destinations. The DCS 3000 can collect ELSUR data under the Pen Register warrants, which are concerned with call data.

Deployed in CMPs throughout the FBI, the DCS 3000 is currently operating under an existing type certification and accreditation from the period of May 28, 2003 to May 27, 2006. This revision of the SSP addresses requirements specified in the 2.1 version of the FBI Certification and Accreditation Handbook for TICTU to renew the certification and accreditation of the system.

1.2.2 Supported Projects

PROJECT NAME	CLASSIFICATION & COMPARTMENTS	PROJECT POC
TICTU	Unclassified but Sensitive	[redacted]

b6 b7C

The DCS 3000 is an ELSUR collection system.

1.2.3 Information System Usage

□ Briefing Boards	□ Network Management	☑ Data Collection
□ Communications	□ Presentations	☑ Data Processing
□ Collaborative Computing	□ Software Development	□
□ Database	□ Prototyping	□
□ Data Release	Signals Processing	□

□ E-Mail	□ Spreadsheets	□
□ Image Processing	□ Web/Web Design	□
□ Mapping	□ Word Processing	□

1.3 Inter-Departmental/Agency Use and Agreements

1.3.1 Joint Use Information

The DCS 3000 is not subject to Joint-Use Agreements.

1.3.2 Memorandum of Agreement (MOA)/Understanding (MOU)

The DCS 3000 is not subject to any MOAs or MOUs.

1.3.3 Interconnection Security Agreement (ISA)

The DCS 3000 system is not subject to any ISAs.

2. SECURE FACILITY DESCRIPTION

2.1 Facility Layout

DCS 3000 systems, deployed at approximately 80 FBI-controlled sites, are located in CMPs in FBI field offices, ERF in Quantico, resident agencies, and task forces around the country. The system may also be deployed at FBI-controlled undercover locations. Access to the FBI facilities is controlled by use of security guards, electronic door locks, visitor badges, and visitor logs.

[redacted]

b2
b7E

[redacted]

b2
b7E

2.2 Physical and Environmental Protection

2.2.1 Physical Protection

[redacted]

b2
b7E

2.2.2 Environmental Protection

Fire alarms systems, sprinkler, and/or Halon systems are used to protect FBI field office personnel, facilities, and equipment from injuries, damage, or loss due to fire.

In the advent of a power failure, FBI field offices have uninterruptible power supplies (UPS) and auxiliary power units to prevent any interruption in organizational activities due to power outage. Electronic surveillance systems would remain operational for many hours after a power failure. In fact, all FBI systems could use power supplied through an auxiliary generator indefinitely as long as its fuel supply could be replenished. Failure of the heating and air-conditioning systems, water, sewage, and other utilities most likely would not have an immediate impact on DCS 3000 activities and could be worked around in most cases. If an FBI field office facility were destroyed due to earthquake, tsunami, windstorm, or to any other natural or manmade event, the DCS 3000 equipment within that facility could be replaced and be operational at an another location within approximately 2 weeks.

Further information on environmental protection is available from the Physical Security reports created by the Physical Security Unit for a given facility.

2.3 System Layout

The DCS 3000 system is located in CMPs in all FBI offices, including field offices and the ERF. Office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus FISA, and computer operations versus case monitoring). Locations of these CMPs vary with the design of the particular FBI offices. Locations of the DCS 3000 equipment within these CMPs vary by individual deployment.

2.4 Emanation Protection

2.4.1 Red/Black Separation

[redacted]

b2
b7E

2.4.2 TEMPEST

The DCS 3000 system is not subject to TEMPEST requirements.

3. SYSTEM DESCRIPTION

3.1 Summary

Summary:

The DCS 3000 system was developed to assist the FBI with collecting and processing data for court-ordered ELSUR operations for criminal and FISA investigations. To conduct court-ordered ELSUR operations, the system connects to switches that are used by TSPs to route telephone calls to their destinations. The DCS 3000 can collect ELSUR data under the Pen Register warrant, which are concerned with call data.

System Architecture/Key Components:

The DCS 3000 application suite consists of six component applications residing on one or more workstations. Not every component application is used during a surveillance operation; individual installations of the DCS 3000 vary according to need. The components of the DCS suite used to support a particular requirement depends upon the type of surveillance to be conducted, the switch providing the data, the TSP, and availability of equipment at the office. The DCS 3000 consists of the following applications:

[redacted]

b2
b7E

Cisco routers are used to connect the DCS 3000 to the TSPs' switches. The separately accredited [redacted]s utilized to connect the various DCS 3000 installations to each other. See Attachment B for a diagram of a typical configuration of the DCS 3000 system.

b2
b7E

[redacted]

b2
b7E

[redacted]

b2
b7E

Perimeter:

The DCS 3000 accreditation boundary is defined to include the router used to receive information from the TSP, DCS 3000 workstations and software. Only hardware and software under the direct control of the FBI are included within this boundary. All other facilities or equipment will be considered as external interfaces.

DOJ 2640-2D, Information Technology Security and the FBI Manual of Investigative Operations and Guidelines (MIOG) prescribe the general technical controls for the DCS 3000 system. These controls are typical of those found in similar U.S. Government IT systems.

User Population:

User access to the DCS 3000 files is closely controlled because of the nature of the data that is collected. Since these files may be used as evidence, participants closely adhere to the FBI guidelines and rules for evidence handling and protection. Though a variety of FBI participants may be present during an operation, only technically trained agents (TTAs) are required to be present during electronic surveillance. Other participants such as translators, intelligence research specialists, and system administrators plan important operational roles during the operation, but generally are not present or needed during electronic surveillance. Participant roles are clearly defined and understood, and these roles are generally exclusive of each other.

The following technical document is maintained at the ERF and at each of the field offices where DCS 3000 is deployed: DCS 3000 User Guide. In addition, the following documents have been generated in support of the FBI C&A effort for the DCS 3000:

- DCS 3000 System Security Plan (this document)
- DCS 3000 Risk Assessment and Management Plan.

Mode of Operation, Levels of Concern (LoC), and Tier Designation:

The DCS 3000 runs in the Dedicated Mode of Operation because all users have all required formal approvals for access and a need to know for all the information on the system. The Confidentiality LoC is set at medium since data passed through the DCS 3000 is collected in support of criminal cases and can be used as evidence. The Integrity LoC is set at medium because data passed through the system must not be altered, lost, or erased either accidentally or surreptitiously since it is collected for possible use as evidence in criminal cases. Loss of Integrity will have an adverse effect on organizational-level interests. The Availability LoC is set at medium since the loss of availability will have an adverse effect on organizational-level interests.

Data Flow and Controls

The DCS 3000 collects call data from the TSP and stores it at the CMP site. [redacted]

b2
b7E

3.2 Mode of Operations

☑ Dedicated	□ Compartmented
□ System High	□ Multi-Level

The Dedicated Mode of Operation has been assigned to the system because all users have all required formal approvals for access to all information on the system, and all users have a need to know for all of the information on it.

3.3 Level of Concern

3.3.1 Confidentiality

□ Basic	☑ Medium	□ High

A medium LoC for system confidentiality is assigned in accordance with the provisions in the FBI Certification and Accreditation Handbook since data that is passed through the DCS 3000 is collected in support of criminal cases and can be used as evidence.

3.3.2 Integrity

□ Basic	☑ Medium	□ High

A medium LoC for system integrity since data passed through the DCS 3000 must not be altered, lost, or erased either accidentally or surreptitiously since it is collected for possible use as evidence in criminal cases. Loss of data integrity by the DCS 3000 will have an adverse effect on organizational-level interests.

3.3.3 Availability

□ Basic	☑ Medium	□ High

The medium LoC rating is based on the degree of ready availability required for the information maintained, processed, and transmitted by the DCS 3000 in order to accomplish the mission of its users. Since the loss of availability will have an adverse effect on organizational-level interests, the DCS 3000 is assigned a medium LoC for availability. This will require that information must be readily available with minimum tolerance for delay, which means that routine system outages do not endanger mission accomplishment; however, extended system outages may endanger the mission.

3.4 Tier Level Designation

□ **Tier 1**	☑ **Tier 2**	□ **Tier 3**	□ **Tier 4**

3.5 System Diagram

The DCS 3000 is connected to the TSP via [redacted] The connection can be established either by the DCS 3000 or by the switch. Data transmitted to the DCS 3000 in support of Pen Register collections is unclassified but sensitive.

b2
b7E

The DCS 3000 is a modular system that can be set up and configured to meet specific case needs. Figure 3, found in Attachment B, presents a typical configuration. Call data is provided from the switch to [redacted]

The DCS 3000 is connected to the TSP[redacted] DCS 5000, DCS 6000, and[redacted] systems. Furthermore, received data is not re-transmitted externally outside of the CMP. b2 b7E

3.6 Interconnection Interface Description

3.6.1 Direct Network Connections

☐ This system does not connect with any other system.

☑ This system connects with the following network(s) or system(s):

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY
DCS 6000 via Pix Firewall	Unclassified but Sensitive	FBI
[redacted]	Unclassified but Sensitive	FBI
[redacted]	Unclassified but Sensitive	FBI
DCS 5000 via CI100, a one-way connection	Secret	FBI
TSP	Unclassified but Sensitive	N/A

b2
b7E

3.6.1.1 Connectivity Management Procedures

Overall:

TICTU enforces procedures for identifying and documenting both external and internal connectivity of the DCS 3000 system. The security support structure includes limitations of physical and logical access to both the DCS 3000 and any other systems connected to it. The DCS 3000 and the other connected systems are deployed to CMPs, which limit access to personnel who require access in performance of their duties. It is assumed the TSPs also limit physical access to their equipment. The DCS 3000 and the other connected systems also limit logical access to the system through the use of identification and authentication mechanisms such as user ids and passwords. It is assumed the TSPs similarly limit logical access to its systems to only certain employees by similar mechanisms. Routers are configured to use static routing to increase protection by only allowing routing to certain networks and access control lists used to block unwanted IP traffic.

See Section 7.2.3 for further information on the DCS 3000 Configuration Management Plan.

External Connectivity:

The DCS 3000 is a system that only receives data from TSPs and transfers data to other systems via dedicated, secure connections.

The local field office or the ERF is responsible for arranging for the connectivity to the TSP. Like other entities, the FBI obtains the dedicated connection from the TSP by providing payment to the TSP in accordance with their policies. To obtain the necessary data, the personnel assigned to the investigation must provide the warrant information to the TSP. The TSP then configures their systems to provide the information to the DCS 3000. However, TICTU provides and tracks the routers necessary to connect the DCS 3000 to the TSP. TICTU and the local technical agents maintain these routers, switches, and their configuration. Routers are statically configured with control lists mitigating the risk of modification by unauthorized personnel or access by unauthorized IP traffic.

Prior to installation, TICTU approves of all non-TSP external connections to all DCS 3000 sites. TICTU also provides the routers, and other equipment necessary for the non-TSP-related external connections listed in section 3.6.1.2 to all sites. TICTU and the local technical agents track and maintain this equipment, including their configuration. Routers are statically configured with access lists like TSP connections.

TICTU authorizes and manages all deployments of the DCS 3000 system. TICTU ensures that all sites are located in CMPs in FBI-controlled spaces that are cleared for Trilogy access. Additionally, TICTU provides all equipment to the other DCS 3000 sites including switches, routers, and workstations. All equipment is preconfigured with static IPs, certified and accredited, and logged into a database prior to shipment. Once installed, TICTU personnel can remotely access all DCS 3000 systems via secure PC Anywhere procedures.

3.6.1.2 Interconnection

DCS 6000 via Pix Firewall: The DCS 3000 connects to the DCS 6000 via a [redacted]. The DCS 6000 system collects and processes Title III call data and content for criminal cases. The system obtains the call data through [redacted] and TSP proprietary messages provided by the DCS 3000. Thus, both the DCS 3000 and the DCS 6000 are equally classified unclassified but sensitive. Since the DCS 6000 systems are located in CMPs, foreign nationals can not access or use the system. The DCS 6000, including the Pix Firewall, is separately accredited by the FBI.

b2
b7E

[redacted] The DCS 3000 utilizes th[redacted]o connect DCS 3000 systems in FBI offices to other DCS 3000 systems found at collection sites, as shown in Figure 3.[redacted] No foreign national users can access or utilize th[redacted] is separately accredited by the FBI.

[redacted] The DCS 3000 connects to the equally classified [redacted] legacy Pen Register collection system [redacted] ke the DCS 3000, the [redacted] ystem cannot be accessed or utilized by foreign nationals. Only [redacted] nd TSP proprietary data are provided by the DCS 3000. The [redacted] s also accredited by the FBI. b2 b7E

DCS 5000 via [redacted] The DCS 3000 connects to the DCS 5000 system, a Secret system for collecting and processing FISA information. [redacted] one-way pipe to a higher classified system through the CI100, which ensures the data only flows from the DCS 3000 to the DCS 5000 system. [redacted] [redacted] Because of the nature of the system's mission, DCS 5000 is neither accessible nor utilized by foreign nationals. The DCS 5000 system is accredited by the FBI. b2 b7E

TSP: The DCS 3000 connects to unclassified but sensitive TSPs via dedicated, secure connections in support of court-authorized collections. These connections, which can be established by either the DCS 3000 system or the TSP switch, are controlled via switches and routers that are statically configured by the SBIT or TICTU teams. Only [redacted] and TSP [redacted]. While no foreign national users are present on the DCS 3000 system, the TSP may employ foreign nationals and provide telephony services to the general public, including foreign nationals. Because the DCS 3000 only connects to TSPs who do not have a Designated Accrediting Authority (DAA), ISAs are not required. b2 b7E

3.6.1.3 Connectivity Procedures

DCS 3000 external connectivity is controlled by the TICTU, SBIT, and FBI office technical agents using standard industry best practices. The DCS 3000 only receives data from TSPs and transfers data to other systems via dedicated, secure connections. The system only provides data to other systems or networks residing within the CMP via a secure connection. All DCS 3000 routers providing external connectivity are statically configured by the SBIT or technical agents at the particular office, utilize access control lists to limit modifications to only authorized personnel and allow only predefined data connections to the FBI DCS 3000 system. External connections are monitored for malicious traffic, which is automatically stopped prior to entering the system. The system only accepts and provides data via a limited number of IP addresses, ports and protocols, decreasing the probability of attacks by internal and external unauthorized entities because application internet protocols such as HTTP and FTP are not used.

TICTU authorizes and manages all deployments of the DCS 3000 system. TICTU ensures that all sites are located in CMPs in FBI-controlled spaces, and are cleared for Trilogy access. Additionally, TICTU provides all equipment to the other DCS 3000 sites including switches, routers, and workstations. All equipment is preconfigured with static Internet Protocol (IP) Addresses, certified and accredited, and logged into a database prior to shipment. Once installed, TICTU personnel can remotely access all DCS 3000 systems via secure PC Anywhere procedures.

Numerous laws, regulations and policies influence the operation and modification of all current information technology systems and the development of new ones. In addition, the development and operation of the DCS 3000 and the conduct of those personnel who are part of its operation have been, and will continue to be, rigidly controlled by the mandates of United States Code 18, *Crimes and Criminal Procedure* (i.e., 18USC2510 et seq., and 3121 et seq.). Virtually every activity associated with an FBI electronic surveillance operation is performed with these requirements firmly in mind. This system and the people who operate it must comply with all legal requirements that this code stipulates for the conduct of every aspect of FBI electronic surveillance operations.

However, the system was developed with a set of security policies integrated into it that help enforce compliance with those requirements during its operation. Finally, personnel who participate in the operation of the system are closely monitored to ensure they comply with this code. These inherent security components of the system itself and its operation collectively provide an additional layer of information security that is not present for the operation of most other information technology systems that handle SBU information.

3.6.1.4 Networking

[redacted]

b2
b7E

3.6.2 Indirect Connections

3.6.2.1 Indirect Import

[redacted]

b2
b7E

Scans would be conducted on any removable media prior to conducting indirect imports using McAfee VirusScan software. See section 7.3.4.1.1 and 6.2 for more information.

3.6.2.2 Indirect Export

[redacted]

b2
b7E

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
Telecommunications Applications (TA) Mainframe		FBI	

Scans are conducted on any removable media prior to conducting indirect exports using McAfee VirusScan software. See sections 7.3.4.1.1 and 6.2 for more information.

3.7 Data Processed

3.7.1 Classification and Compartments

☑ UNCLASSIFIED	□ SI	□ Other:
□ CONFIDENTIAL	□ TK	□ Other:
□ SECRET	□ HCS	□ Other:
□ TOP SECRET	□ G	□ Other:
	□ Q	□ Other:

3.7.2 Dissemination Controls

□ Originator Controlled (ORCON)	□ Rel To:
□ Sources And Methods Information (SAMI)	□ Rel To:
□ Not Releasable To Foreign Nationals (NOFORN)	□ Other:
X Sensitive But Unclassified	□ Other:
☑ For Official Use Only (FOUO)	□ Other:
□ Law Enforcement Sensitive (LES)	□ Other:

3.7.3 Type of Data Processed

The DCS 3000 system processes Criminal Investigative Information (CII) where the case agents are considered the Data Owners and Data Managers.

3.8 Data Flow Diagram

b2
b7E

The DCS 3000 collects data from the TSP and stores it at the CMP site. Figure 1 shows the internal flow of data through the DCS 3000. Call Data Channel (CDC) data is provided by the TSP. [redacted]

[redacted]

b2
b7E

Figure 1: DCS 3000 Data Flow

4. SYSTEM HARDWARE

4.1 Hardware List

A list of hardware used in the DCS 3000 system is provided in Table 1. See Attachment C for a site-specific hardware list.

Nomenclature	Model	Manufacturer	Memory-Component	Serial Number	Location
External Modem	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Router	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Workstations	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

b2
b7E

Table 1: Equipment List

The DCS 3000 can be installed on any Pentium-based workstation running Windows 2000 or Windows 2003. The minimum memory requirements are the same as the minimum required for running the operating system.

4.2 Hardware Labeling

4.2.1 Labeling of System Hardware

FBI-approved labels commensurate with the classification of the DCS 3000 system are affixed to routers, modems, workstations and monitors by each site. These labels indicate the distribution limitations and handling caveats of the information commensurate with the DCS 3000.

4.2.2 Exceptions

Keyboard, mice and other peripheral devices are not labeled in accordance with FBI policy and procedures.

4.3 Sanitization and Destruction

FBI evidentiary files are stored for at least 12 years regardless of the disposition of the case for which they were generated. However, there are procedures for the destruction of evidentiary information that is less than 12 years old. Also, in the event a hard drive or other removable-media disk with case data on it must be destroyed, its destruction will be done by physically smashing it with a blunt instrument such as a hammer. This method of destruction, as well as those methods required to destroy other forms of evidentiary information are in accordance with the guidelines provided in the FBI Manual of Administrative Operations and Procedures (MAOP), Title 44, U.S. Code, Sections 3303 and 3303a; Title 36, Code of Federal Regulations, Part 1220; the General Records Schedule (GRS); and the FBI Records Retention Plan and Disposition Schedule (The Plan) developed by the National Archives and Records Administration (NARA) and the FBI, which was approved by the United States District Court, District of Columbia, Washington, D.C., September 9, 1986.

Sanitization and destruction of remaining volatile and nonvolatile components is accomplished via official FBI policy and procedures.

4.4 Custom-Built Hardware

The DCS 3000 does not utilize custom-built hardware.

5.0 SYSTEM SOFTWARE

5.1 Software List

The software used by the DCS 3000 system is listed in Table 2.

b2
b7E

Name	Version	Manufacturer	Intended Use or Function
DCS 3000	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
VirusScan	[redacted]	[redacted]	[redacted]
Windows 2000 Workstation	[redacted]	[redacted]	[redacted]
Windows 2003	[redacted]	[redacted]	[redacted]

b2
b7E

Table 2: DCS 3000 Software

DCS Application Component	Version
[redacted]	[redacted]

b2
b7E

Table 3: DCS 3000 Application Version Numbers

Where possible, DCS 3000 systems utilize FBI standard configurations of the Windows Operating Systems and other software. Active Directory is not used in the DCS 3000 systems.

5.2 Software with Restricted Access or Limited Use Requirements

The DCS 3000 was developed as a software tool to support the FBI's collection of court-authorized surveillance data. The FBI is in charge of designing and developing all DCS 3000 software, with significant support from contractor personnel. A prototyping methodology is employed, with the priority of meeting immediate law enforcement collection needs. The requirements for each software change are reviewed by technical personnel and approved by the DCS 3000 Project Manager. After approval, the requirements for each release are documented and provided as release notes, with user-relevant information provided as user documentation. All software changes are documented in the DCS 3000 source code as well as in the release notes.

The FBI owns all rights to the DCS 3000 software suite. Operating system and commercial-off-the-shelf (COTS) software packages, when utilized, are purchased and licensed in accordance with FBI and departmental policies.

5.3 Foreign Software

No foreign software is used in the DCS 3000 system.

5.4 Freeware/Shareware/Open-Source Software

The DCS 3000 system does not utilize freeware, shareware, or open-source software.

5.5 Marking and Labeling

All system software used to install the operating system, DCS 3000 application, and other software are considered unclassified, and are marked accordingly. The DCS 3000 application is only available through TICTU, who provides the application to the other FBI offices. The operating system and other software on the system are available commercially.

6. DATA STORAGE MEDIA

6.1 Media Type

The DCS 3000 system uses hard drives as the primary non-removable data storage media. These hard drives are labeled and controlled in accordance with FBI policy and procedures appropriate to the type of data (Pen-register) found on the system.

TYPE OF MEDIA	SECURITY CONTROLS
Various	In Accordance with FBI policy and procedures for type of data found on system.

Removable Media

TYPE OF MEDIA	SECURITY CONTROLS
Hard Drives	In Accordance with FBI policy and procedures for type of data found on system.

Non-Removable Media

6.2 Media Handling

The DCS 3000 system can record evidentiary data to removable media, namely floppy disks and CDs. Evidentiary data is recorded to a disk as a working copy and to another as an evidentiary copy. Because changes are not permitted to evidentiary data, write-protect mechanisms are used to ensure that data on the evidentiary copy is not modified, removed or tampered with. Each disk is labeled in accordance to the type of data found on the media, and controlled by the suitable FBI processes and procedures. All written documents, tapes, floppy disks, and other removable media generated in support of a case are labeled, stored, transported, and transferred according to every prescribed and strictly enforced FBI procedures. Removable and Non-removable media with evidentiary data are secured when not in use or when housed in a facility not cleared to house this type of data.

Access to ELSUR data is rigidly controlled and governed by various mandates of U.S. Code 18, *Crimes and Criminal Procedure*. Unauthorized access to evidentiary data or to the DCS 3000 system is highly unlikely due to the tightly controlled nature of the workplace in which surveillance operations are conducted. Numerous and varied security measures are in place both physically and electronically to discourage, and in most cases, to prevent such inappropriate activity.

6.2.1 Media Introduction and Removal

Information stored on the DCS 3000 and on removable media is purged of sensitive data in accordance with local procedures established at each CMP. Data storage media are moved into and out the facilities in accordance with local procedures established at each CMP and with procedures in accordance with rules and regulations regarding evidentiary data. Procedures for copying, reviewing, and releasing investigation information will be in accordance with the FBI MIOG.

6.2.2 Sanitization and Destruction

FBI evidentiary files are stored for at least 12 years regardless of the disposition of the case for which they are generated. However, there are procedures for the destruction of evidentiary information which is less then 12 years old. Also, in the event a hard drive or other removable media disk with case data on it must be destroyed, its destruction will be done by physically smashing it with a blunt instrument such as a hammer. This method of destruction, as well as those methods required to destroy other forms of evidentiary information are in accordance with the guidelines provided in the FBI MAOP, Title 44, U.S. Code, Sections 3303 and 3303a; Title 36, Code of Federal Regulations, Part 1220; the GRS; and the FBI Records Retention Plan and Disposition Schedule (The Plan), developed by the NARA and the FBI, which was approved by the Unites States District Court, District of Columbia, Washington, O.K.,, September 9, 1986.

6.3 Storage Media Marking and Labeling

All written documents, floppy diskettes, and other removable media generated in support of a case are labeled, stored, transported, and transferred according to very clearly prescribed and strictly enforced FBI procedures. The classification level, compartments, handling controls, and information contents are labeled on the media as appropriate and directed by FBI policy and procedures. Write protect mechanisms are employed as appropriate to ensure the information contained on the media is not altered or removed.

7. SECURITY CONTROL REQUIREMENTS

7.1 Management

7.1.1 Risk Assessment

The DCS 3000 system is "closed" meaning outsiders cannot gain access to it without defeating multiple layers of physical and electronic security. This multiple-layer approach to information system security is known as "defense-in-depth." Each layer protects the system in a unique way or supplements other layers so a single failure will not compromise the entire system. Since DCS 3000 only receives data from TSPs through controlled interfaces and only provides data to outside networks located in the same CMP, would-be intruders cannot gain access to it electronically by employing known hacking tools and methods. An outside intruder would have to defeat the physical security in place at the CMPs (e.g., Guards, locks, electronic ID badge recognition systems, electronic sensors, system personnel, etc.) in order to gain physical access to the system, and then the intruder would have to break into the system electronically by inserting user IDs and passwords or by employing other hacker methods. Such an effort would not only be highly risky and time-consuming but also be easily detected.

As with most information systems, the greatest threat to the DCS 3000 would come from the inside. Since they have access to the system at various levels, users could damage, alter, or erase data and destroy system hardware and software. They also could use the information gathered by it for profit by passing on the collected information or by alerting those being monitored. The FBI people involved in ELSUR cases have undergone a very thorough screening process in order to work in the FBI, and many of these same people are involved in one way or the other in closely monitoring their own ELSUR operations.

The DCS 3000 is not connected to any external networks, and is therefore not vulnerable to Internet threats.

7.1.2 Compliance and Monitoring Program

A risk assessment for the DCS 3000 system is conducted prior to system certification and accreditation. The methodology used to identify the threats and vulnerabilities of the system may include the use of an in-house or disinterested-party automated risk assessment or may be a simple analysis of the known threats and vulnerabilities associated with the system conducted either in-house by the ISSO or by an outside disinterested investigator. Regardless of the methodology employed, a risk assessment report is generated that will document the results of the automated risk assessment or analysis. This report is marked commensurate with the information contained in it and will be kept by the ISSO or Special Agent in Charge (SAC) in a locked cabinet. The risks identified in this analysis and those described in this security plan are presented to the FBI Chief Information Officer (CIO)/DAA in the form of a risk assessment and management plan. He or she uses this plan in their accreditation deliberation for this system. The following are the DCS 3000 risk assessment policies:

- A risk assessment and analysis must be performed not less than every 3 years.
- Vulnerabilities found during any analysis are corrected or accepted as uncontrolled risks by the SAC or other designated responsible individual. If the decision is to accept a risk that was found during a risk analysis/assessment, then the decision is

documented as an uncontrolled risk and signed by the Senior Agent in Charge (SAIC) or other designated responsible individual.

- The risk analysis questionnaire and associated correspondence are considered sensitive documents and appropriately labeled, handled, and filed in a locked cabinet. These sensitive documents are:
  - Maintained by an individual designated in writing, along with the risk analysis report and must be available for review by authorized FBI IA representatives when required.
  - Intended for completion by the facility ISSO or other qualified designee.

In accordance with version 2.1 of the FBI Certification and Accreditation Handbook, the ISSO will conduct a review of the DCS 3000 system security annually when the system is not undergoing the certification and accreditation process. The resulting report is classified commensurate with the information contained in it and will be kept by the ISSO or the SAC in a locked cabinet. The ISSO ensures that any anomalous findings from the test will be mitigated appropriately and regression testing performed. Results from the ISSO's annual review are provided to the SecD certification unit and accreditation unit upon request.

Vulnerabilities identified in the risk assessment, certification and accreditation process, and the annual testing are reviewed and mitigation strategies commensurate with the value of the system and data identified. Once these mitigation strategies are developed, the Plan of Action and Milestones (POA&M) is revised to include a schedule of implementation.

The system was developed with a set of security policies integrated into it that help enforce compliance with those requirements during its operation. Finally, the personnel who participate in the operation of the system are closely monitored to ensure they comply with this code. These inherent security components of the system itself and of its operation collectively provide an additional layer of information security that is not present for the operation of most other IT systems that handle SBU information.

7.2 Operational

7.2.1 Personnel Security

All FBI positions have been reviewed for sensitivity level. Prior to their employment with the FBI, all individuals must have an FBI top-secret clearance with associated background investigation.

FBI clearances are updated every 5 years with the exception of those of language specialists who are re-evaluated yearly to include Personnel Security Interviews (PSI). For personnel who want to be special agents for the FBI, the screening and adjudicative processes for obtaining an FBI top-secret clearance are interrelated and quite comprehensive. For the purposes of this document, they will be considered as one combined process. A prospective FBI special agent (i.e., applicant) begins both these processes by completing and submitting an FD Form 646, FBI Preliminary Application for Special Agent Position, (or applying on-line) and then satisfactorily completing Phase I (i.e., Biodata Inventory, Cognitive Ability, and Situational Judgment) testing. At this point, the applicant will fill out an FD Form 140, FBI Application for Employment, and will undergo Phase II testing which consists of a structured interview and a written exercise. After successfully completing Phase II testing, the applicant will enter into the Final Screening Process in which he or she will:

- Receive a Conditional Letter of Appointment
- Participate in a PSI
- Receive a polygraph examination
- Undergo drug testing
- Undergo a background investigation
- Receive a pre-employment physical examination

Data that is collected from all these personal tests, interviews, examinations, and investigations are then compiled and analyzed by personnel from the Bureau Applicant Employment Unit of the Administrative Services Division. A "hiring brief" is then developed on the applicant for project manager (PM) review with subsequent delivery to the personnel in the Personnel Security Section/Re-Investigation Unit of the Security Division for their review and recommendation. After they have completed their review and made their recommendation, they return the hiring brief to the PM from whom it came for his or her final review and Hire or No-Hire decision. Once the SA applicant has been hired, he or she will be granted an FBI Top Secret clearance and will join other classmates for extensive training at the FBI Academy.

For potential non-SA (i.e., support) new hires, the screening process is no less comprehensive than that of a prospective SA. The applicant applies for a support position/vacancy shown on-line through the FBI web page. This electronic application not only includes those entries required on the FD Form 646, but also requests information specific to the vacancy for which the applicant is applying. The Administrative Support Division/Staffing Unit reviews the support applicant's submission and determines if he or she satisfies the knowledge, skills and abilities (KSA) required for the job. If so, the applicant may be required to take a test to determine his or her suitability for the work they will be doing. For instance, someone applying for an FBI secretarial position would have to pass a test that demonstrated that person's secretarial abilities were sufficient for the job. If the applicant passes the test or if no test is required for that particular position/vacancy, but the applicant has the KSAs for the job, he or she will be asked to complete an FD Form 140 and bring it with them for submission to an interviewer during a scheduled interview. After completion of a successful interview, the Background Process (i.e., very similar to an SA applicant's Final Screening process) begins. From this point on, the administrative and adjudicative processing of support applicant data is identical to that for an SA candidate.

Processing time for both SA and support applicants ranges anywhere from 4 to 8 months.

Approval to access the CMP and any ELSUR information is performed by each site in accordance with local policy and FBI procedure.

7.2.1.1 Non-U.S. Citizens

No non-U.S. Citizens has access to the DCS 3000.

7.2.2 Contingency Planning

7.2.2.1 System Backup

<u>Protections of the backup and restoration hardware, software, and firmware:</u>

Since the DCS 3000 does not utilize any unique hardware, the systems components are readily replaceable. The DCS 3000 application components can utilize most COTS workstations as long as they support the Windows 2000 Workstation or the Windows 2003 Operating System. These workstations are readily available. TICTU maintains an inventory of spare modems, routers, hard drives and workstations. In the event that spares are not available, these hardware devices are commercial products readily obtained in a short period of time.

TICTU procures, configures, and maintains all hardware utilized in the DCS 3000 systems. TICTU configures the DCS 3000 workstations with [redacted] If one hard drive no longer functions, the system will still operate using the other disks without any information loss. The system will function, allowing the broken hard drive to be replaced. b2 b7E

TICTU ensures that copies of the software, firmware, service packs, patches and virus definitions are easily obtainable when needed. Copies of the software are stored on CD or other media in a secure location. This location is readily accessible to the system administrators. The DCS 3000 installation package is available on the FBINET and on CD. However, TICTU controls who has the applications and the number of instances of the DCS 3000 application software via an authorization code required during installation. This authorization code can only be obtained from TICTU.

The DCS 3000 provides a capability to conduct backup storage and restoration of data and access controls. The DCS 3000 backup capability provides for the restoration of any security-relevant segment of the system state (e.g., access control lists, deleted system status information) without requiring destruction of other system data. All backups are securely stored in a locked file cabinet by the ISSO or the system administrator in the local CMPs until needed.

<u>Backup Program Procedures:</u>

Backups are an important part of the ability to recover fully and quickly in the event of a failure on the DCS 3000. However, not all information on the DCS 3000 needs to be backed up; only the router configurations, modem configurations, and data residing on DCS 3000 application components requires backup. The operating system, software, patches, service packs, and virus definitions are available as described above.

Backups of all router and modem configurations should occur during initial installation and after any modifications to the configurations take place. A minimum of the last two configurations of any router or modem are maintained to ensure in case the latest copy has a bug in it. Also, two copies of each of the backups are maintained in case of corruption or loss of one of the copies.

Backups of the DCS 3000 application components is performed using the backup and restoration mechanism provided by the Windows 2000 Workstations or Windows 2003

Operating Systems. The software is configured to capture any data, logs, account information and other security-relevant information on the system. System components are backed up a minimum of once per month when not in use for ELSUR. When capturing ELSUR data, the application components are fully backed up weekly with daily incremental backups performed. Two copies of each backup are maintained in case of corruption or loss of one of the copies. These copies are maintained for three years or the amount of the time required by appropriate FBI policy, whichever is greater.

7.2.2.1.1 Backup Protection

All DCS 3000 equipment, software, and media are physically located in secure CMPs.

The FBI offices securely store the official media for the operating system and the DCS 3000 system. The system administrator or ISSO can access these media when necessary to restore the system.

The DCS 3000 provides a capability to conduct backup storage and restoration of data and access controls. The DCS 3000 backup capability provides for the restoration of any security-relevant segment of the system state (e.g., access control lists, crypto-logic keys, deleted system status information) without requiring destruction of other system data.

7.2.2.1.2 On-site & Off-site Storage

[redacted]

b2
b7E

7.2.2.2 Telecommunications Services

[redacted]

b2
b7E

7.2.2.3 Backup Power Supply Requirements

[redacted]

b2
b7E

7.2.2.4 Recovery Procedures

7.2.2.4.1 Continuity of Operations Plan

In the event of a failure on a DCS 3000 system, the administrator can configure another system to receive the data while the other system is repaired. Administrators or technicians diagnose the problem with the particular device before resolving the problem. In the event of a suspected security incident, the procedures noted in the section 7.2.7 are followed before attempting to resolve the situation. In all other events, a probable cause for the failure is determined and appropriate actions, such as changing the configuration or adding a patch, are taken to avoid similar situations in the future.

If a catastrophic failure occurs to any of the DCS 3000 components, recovery can be accomplished by rebuilding the particular device. Routers and modems can be restored by adding the configuration, available on backups, to a router with the proper firmware and version of the IOS. For the DCS 3000 applications, the system administrator can rebuild a workstation with Windows 2000 workstation, the application, Virus Scan, and other software and patches required. Any data and other information can be added to the system using the recovery mechanisms provided in Windows 2000 workstation from available backups. Prior to performing recovery, a virus scan will be conducted on the backup media.

Each FBI location has written and coordinated comprehensive system security contingency plans, which include DCS 3000 systems, to cover the loss of equipment, personnel and data due to unforeseen calamities at FBI office locations such as fire, earthquake, flood, wind, etc. These plans are tailored to match the environments within which each individual system operates.

7.2.2.4.2 Disaster Recovery Plan

Not applicable to the DCS 3000 system.

7.2.3 Configuration Management Program

Overall:

TICTU's CM process for the DCS 3000 is overseen by a Configuration Management Control Board (CMCB), which supervised by the ISSO and consists of technical personnel. All major changes in hardware, software, and documentation go through the following processes and are approved by the CMCB. TICTU maintains a database in the ERF that tracks all hardware, software, and documentation for every DCS 3000 system (review of the database is available upon request). Change control is enforced by TICTU's procurement process and system administrators using PC Anywhere to confirm the configuration of their systems. TICTU validates and verifies each system before being shipped. Additionally, the DCS 3000 system is subject to the Compliance Monitoring Program detailed in section 7.1.2. Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware and software are available in sections 7.2.2.1 and 7.2.2.4.

Hardware:

TICTU maintains a baseline of the DCS 3000 equipment and is responsible for providing all DCS 3000 hardware at all locations where the system is deployed. Any major changes to hardware, including hardware upgrades, are proposed to the CMCB and must be approved by the board prior to deployment. The CMCB ensures that all proposed changes to the current DCS 3000 hardware configuration meet the appropriate user, system, network, and security requirements prior to deployment. The CMCB also ensures efficient hardware maintenance, deployment and upgrade strategies are followed.

Software:

TICTU maintains the baseline of all software on all DCS 3000 systems, including the operating systems, IOS, virus scanners, remote control applications, and the DCS 3000 application. Any major changes to the software baseline, including upgrades, are proposed to the CMCB and must be approved by the board prior to deployment. The CMCB ensures that all proposed changes to the current DCS 3000 software configuration changes meet the appropriate user, system, network, and security requirements prior to deployment. The CMCB also ensures efficient software maintenance, deployment and upgrade strategies are followed. System administrators monitor the configuration of DCS 3000 systems remotel[redacted] [redacted]

b2
b7E

TICTU controls the DCS 3000 application via an authorization code, which is required when installing any of the components. When issuing the authorization code, TICTU notes the person requesting the code, the code itself, the date and the location.

Documentation:

DCS 3000 documentation is revised on an as needed basis to cover any major changes to the system. The revised documentation is reviewed by the CMCB to ensure correctness and is distributed to the community at large via FBINET or hard copy. Softcopies of the documentation are posted to the FBINET for easy accessibility.

7.2.3.1 Hardware & Software Procurement

The DCS 3000 application was developed as a software tool to support the FBI's collection of court-authorized surveillance data. The FBI is in charge of designing and developing all DCS 3000 software, with significant support from contractor personnel. A prototyping methodology is employed, with the priority of meeting immediate law enforcement collection needs. The requirements for each software change are reviewed by technical personnel and approved by the DCS 3000 Project Manager. The Project Manager is also the ISSO for the system. After approval, the requirements for each release are documented and provided as release notes, with user-relevant information provided as user documentation. All software changes are documented in the DCS 3000 source code as well as in the release notes.

The FBI owns all rights to the DCS 3000 software suite. Operating systems and COTS software packages are purchased and licensed in accordance with FBI and departmental policies. Likewise, all hardware is purchased in accordance with FBI and departmental policies.

7.2.3.2 Evaluation

The FBI owns all rights to the DCS 3000 software suite. Operating systems and COTS software packages are purchased and licensed in accordance with FBI and departmental policies. The CMCB evaluates all software for security impacts prior to approving it for release on the DCS 3000 system. Where possible, FBI standard configurations of the operating system and other software are used.

7.2.4 Maintenance

7.2.4.1 Maintenance and Repair Procedures

b2
b7E

TICTU provides on-call maintenance support of fielded systems. These personnel can also access and assist sites via the tightly controlled [redacted] application residing on the system. In the event that replacement parts or devices are necessary, TICTU personnel pre-configure the components prior to shipment. The personnel then walk site personnel through procedures for replacing the component. In the case of major programs, TICTU personnel may visit the site to repair the problems. Onsite personnel do not fix the systems without TICTU support.

7.2.4.2 Maintenance Procedures Using Uncleared Personnel

The DCS 3000 is operated in FBI-controlled spaces with cleared personnel. No uncleared or lower cleared personnel are used to perform maintenance on the DCS 3000 system.

7.2.4.3 Maintenance Logs

The DCS 3000 is maintained only by TICTU personnel. These personnel track the maintenance on all DCS 3000 systems via the CM database or audit logs on the systems, which include information on the date and time of the maintenance, the type of maintenance performed, and possibly who performed the maintenance. The CM database tracks any replacement parts shipped to the site, which system received the parts, and the date of the maintenance was performed. When necessary, the ISSO reviews the information in the CM database and audit logs. This information is available upon request.

7.2.4.4 Hardware & Software Maintenance

7.2.4.4.1 System Start-Up/Shut-Down

Startup Procedures:

[redacted]

b2
b7E

Shutdown Procedures:

[redacted]

b2
b7E

[redacted]

b2
b7E

7.2.4.4.2 Security Controls and Operations during Maintenance

The DCS 3000 is located in CMPs in all FBI offices. These areas are strictly controlled in accordance with FBI policy and procedures (see Section 2 for more detail). All maintenance and repairs are performed by qualified, cleared personnel.

7.2.4.4.3 Remote Diagnostics

The SBIT team utilizes [redacted]o remotely control the DCS 3000 systems deployed in the ERF and the other locations for maintenance and repair purposes. The usernames and passwords used on the system are strictly controlled and only provided on a need-to-know basis [redacted] configured to utilize the security mechanism available with the software, including the [redacted] mechanism and other security mechanisms.

b2
b7E

7.2.4.4.4 Hardware & Software Transfer, Relocation, and Release

Procedures for moving sensitive computer hardware and data storage media into and out of the CMP are in accordance with local procedures established at each CMP. Procedures for copying, reviewing and releasing investigation information will be in accordance with the FBI MIOG.

7.2.5 System & Information Integrity

7.2.5.1 System Integrity

7.2.5.1.1 System Start-up

See section 7.2.4.4.1.

7.2.5.1.2 After Hours Processing Procedures

The DCS 3000 application requires the DCSAdmin user to be logged on to the system in order to operate. In the event After Hours Processing is required, any personnel required for the ELSUR follow the appropriate policies and procedures for their particular facility. The DCS 3000 system does not require any special controls for After Hours Processing.

7.2.5.2 Data and Software Integrity

7.2.5.2.1 Data and Software Integrity Procedures

The DCS 3000 was developed as a software tool to support the FBI's collection of court-authorized surveillance data. The FBI is in charge of designing and developing all DCS 3000 software, with significant support from contractor personnel. A prototyping methodology is employed, with the priority of meeting immediate law enforcement collection needs. The requirements for each software change are reviewed by technical personnel and approved by the DCS 3000 Project Manager. After approval, the requirements for each release are documented and provided as release notes, with user-relevant information provided as user documentation. All software changes are documented in the DCS 3000 source code as well as in the release notes.

Though the use of integrity mechanisms is required for systems that have a medium level of concern for data and system integrity, the system is not connected to any outside system or network and does not transmit data externally. Because of these mitigating factors, it is considered at very low risk for external data or file tampering. Though the insider threat to this system is considered much higher than the external threat, it is considered minimal due to the tight physical, personnel, and systemic controls inherent to ELSUR operations. The inherent capabilities of the DCS 3000 operating system are used for password protection. Future versions of the DCS 3000 applications will [redacted] b2 b7E

7.2.5.2.2 Data Copying, Reviewing, and Release Procedures

DCS 3000 information is stored in the CMP, an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per week operational area. Data is not transmitted out of the CMP. Procedures for moving sensitive data storage media and computer hardware into and out of the CMP will be in accordance with local procedures established at each CMP. Procedures for copying, reviewing, and releasing investigation information will be in accordance with the FBI MIOG.

The DCS 3000 uses modems and routers to provide connectivity between the ERF and TSPs. Routers will be configured to use static routing (manually adding routes in each router's routing table) to increase protection by only allowing routing to certain networks.

See section 6.2.1 "Media Introduction and Removal" for further information.

7.2.5.2.3 Printout/Hardcopy

All written documents generated in support of a case are labeled, stored, transported, and transferred according to very clearly prescribed and strictly enforced FBI procedures.

7.2.5.2.4 Non-Repudiation

Not applicable for the DCS 3000 system.

7.2.5.2.5 Transaction Rollback

Not applicable for the DCS 3000 system.

7.2.6 User's Guides

7.2.6.1 Configuration Guides

The following guides are used to configure the DCS 3000 system:

- DCS 3000 Users Guide, providing information for the DCS 3000 application.
- FBI-approved versions of Windows 2000 and Windows 2003 operating systems.
- FBI-provided configuration guides for routers, switches, and modems.

7.2.6.2 Guides for Privileged Users

Not applicable to the DCS 3000 system.

7.2.6.3 Guides for General Users

TICTU provides a DCS 3000 Users Guide to all users of the system at all sites. This guide is available through the TICTU contacts listed in Section 1.1.2 or on the FBINET.

7.2.7 Incident Response

DCS 3000 personnel must follow the reporting guidance provided in the FBI MIOG, Part 2, Section 35, and DOJ 2640.2D, Section 5. This guidance provides the user with basic information on when and who to notify if a security incident has occurred or is suspected. All security incidents, whether real or suspected, must be reported to the unit ISSO or to the next higher security-level representative. That person will evaluate each incident to determine if it has system or even broader FBI IT implications. If the ISSO decides that an incident does have system or FBI-wide implications, he or she will notify the FBI ADP Security Officer as required. Then, the FBI will use this information to determine the extent of the reported incident and what needs to be done to resolve it.

A major factor the FBI considers during its incident determination process is the criticality of the system for which an incident is reported. Each FBI IT system or major application has been developed to satisfy a specific Bureau need. The degree of criticality for an FBI system or major application is based on how much it is needed and what the repercussions would be regarding FBI operations if it were to fail. If system failure means significant degradation in an essential FBI operation, then any security incident involving that system would warrant an immediate response by the FBI ADP Security Officer and, perhaps, by the FBI Computer Emergency Response Team (CERT). Incidents that could result in such a response include:

- Unexpected or unexplained system crashes
- Mysterious new user accounts that bypass standard procedures
- Sudden high activity on an account that has had little or no activity for months
- Appearance of new files with novel or strange names, accounting discrepancies
- Changes in file lengths or modification dates
- Attempts to write to system files
- Data modification or deletion
- Denial of service
- Unexplained poor system performance
- Suspected virus infection (Immediate CERT notification required!)
- Anomalies
- Suspicious probes
- Suspicious browsing

It is imperative that DCS 3000 operation proceeds uninterrupted from start to finish. This is to ensure that all court-authorized ELSUR data is collected. The likelihood is very low that a security incident, which would cause an interruption in case operations, would occur during the conduct of any DCS 3000 operation. However, the possibility must be considered, and case personnel at all levels must understand what they are to do if a security incident is suspected or observed. This understanding comes from an aggressive and activity-focused unit security-training program that is administered and subsequently documented on a scheduled basis.

7.3 Technical

7.3.1 Access Control

7.3.1.1 Discretionary Access Control (DAC)

Not applicable because the DCS 3000 functions in the dedicated mode of operation.

7.3.1.1.1 Need-To-Know Controls

Not applicable to the DCS 3000 system.

7.3.1.2.1 Internal Marking

All written documents, tapes, floppy diskettes, other removable media and non-removable media generated in support of a case are labeled, stored, transported, and transferred according to very clearly prescribed and strictly enforced FBI procedures.

7.3.1.3 Technical Access Control Mechanism

The DCS 3000 system has a number of effective logical access controls that are used to authorize (or restrict) the activities of system users at all levels. These include hardware and software features that are designed to:

- Permit only authorized access to or within the system
- Detect unauthorized activities

As one of these logical access controls, the FBI requires that an FBI Standard Warning Banner be displayed on all FBI computer monitors (including those of the DCS 3000) prior to log on.

The following logical access controls are found in the DCS 3000 system:

- FBI Log On Banner is displayed prior to log on.
- Vendor-supplied and default passwords are replaced upon installation of system hardware and software.
- User accounts disabled for 30 minutes after 4 unsuccessful access attempts.
- Host-based authentication is used.
- Access to system security software is restricted to system administrators.
- Information access is restricted at the logical view (or field) level.
- Trusted interactions with internal and external entities are restricted.
- FBI policy applies to all data collected through the DCS 3000 system.

Due to the evidentiary nature of ELSUR data that it is collected through it, the DCS 3000 is always in operation during the surveillance phase of a case; therefore user access to all systems must be continuous. Though users may not be actively participating in case activities, they must have immediate access to the DCS 3000 at all times throughout the case surveillance period.

7.3.1.4 User Group and Access Rights

7.3.1.4.1 User Groups

☑ *Users and administrators are not assigned to groups; all UserIDs are at the same level.*
[redacted]
□ *All administrators are assigned to a privileged users group; the privileged users group is different than the general users group.*
□ *All users are assigned to the same group. This group has fewer privileges/access rights than the privileged user group.*
□ *Users are assigned to different groups depending on need-to-know and work assignments.*
□ *User groups have different privileges/access rights depending on need-to-know and work*
□ *Other:* ____________________

b2
b7E

The DCS 3000 utilizes a single user class with administrative rights for all ELSUR Operations.

7.3.1.4.1.1 Privileged User Group Roles

This section is not applicable to the DCS 3000 system.

7.3.1.4.1.2 General User Group Roles

This section is not applicable to the DCS 3000 system.

7.3.1.4.2 System Access Rights

7.3.1.4.2.1 Local System Access Rights

□ *Users cannot set the system access rights of other users.*
☑ *Users can set the system access rights of other users. (Explain below)*

All DCS 3000 systems have only two accounts: DCSAdmin and ERFAdmin. The DCS 3000 system runs using the DCSAdmin account. The ERFAdmin account is used to unlock the DCSAdmin account when necessary, and cannot run the software. Both of these accounts are system administrator accounts, and can change therefore can change the access rights of the other account. Knowledge of the userids and passwords of these accounts is kept on a strict need-to-know basis. The passwords on these accounts vary according to site.

7.3.1.4.2.2 Remote System Access

Remote system access is accomplished through the [redacted] application.

b2
b7E

7.3.1.4.2.3 Non-Data File Access

☐ *Users cannot change the configuration and/or content of any files other than data files*
☑ *Users can change the configuration and/or content of files other than data files. (Explain below)*

The DCS 3000 system contains only two accounts: DCSAdmin and ERFAdmin. Both of these accounts have administrative rights, and therefore can change configuration and/or content of files at will. Knowledge of the usernames and passwords of these accounts is kept on a strict need-to-know basis. TICTU trains system users to contact TICTU regarding any necessary changes to the system. Users of the DCS 3000 system are trained in FBI evidentiary procedures and know they are not permitted to change ELSUR data.

7.3.1.4.3 Privileged Users Access Rights

The DCS 3000 system contains only two accounts: DCSAdmin and ERFAdmin. Both of these accounts have administrative rights. Knowledge of the usernames and passwords of these accounts is kept on a strict need-to-know basis. The DCS 3000 uses the Windows auditing mechanisms and the [redacted] application to monitor and record system–level accesses and console activities. All users of the system are trained to avoid unauthorized access, modification, and deletion of the audit logs by both TICTU and the FBI's computer security training program.

b2
b7E

7.3.1.5 Unsuccessful Logon Attempts

7.3.1.5.1 Log-on Error Handling

If a user enters the wrong UserID or password:

☑ *A* ***30-minute*** *time-out interval is enforced after a maximum of* ***4*** *attempts and* ***disabling*** *occurs when the maximum is reached.*
☐ *Nothing happens. The user can try to log on as many times as he or she wishes.*

□ *Other:*	

7.3.1.5.2 Account Lockout Handling

If a user's account is locked out due to excessive invalid logon attempts, who is authorized to reinstate the user's account?

□ System	□ Privileged User
□ ISSO	□ Account owner
□ Privileged User	□ Any system user
☑ System automatically reinstates the account after a **30 minute** time period.	
Other:	

7.3.2 Identification & Authentication

User access to DCS 3000 files is closely controlled because of the nature of the data that are being collected. Since these files may be used as evidence, ELSUR participants closely adhere to the FBI guidelines and rules for evidence handling and protection. Though a variety of FBI participants may be present during an operation, only TTAs are required to be present during an electronic surveillance. Case agents, though not required to be present during a monitoring session, often are on hand in the field office. Other participants such as translators, intelligence research specialists, and system administrators play important operational roles during the operation but, generally, are not present or needed during an electronic surveillance.

7.3.2.1 System Users

7.3.2.1.1 General Users

□ *All users have their own unique UserID and unique password.*
☑ *Some users share a UserID and password. (Explain below)*
□ *Some users share a password. (Explain below)*
□ *Privileged users with remote access to the system use strong authentication (Explain below)*

The DCS 3000 systems employ only two accounts: DCSAdmin and ERFAdmin. Both of these accounts have administrative rights on the local system. The DCSAdmin is used to run the DCS 3000 application, which must operate 24 hours a day, seven days a week. The ERFAdmin is used to unlock the DCSAdmin account when necessary. The passwords for these accounts are kept on a strict need-to-know basis.

7.3.2.1.2 Privileged User

□ *All privileged users have their own unique UserID and unique password.*
☑ *Some privileged users share a UserID and password. (Explain below)*
□ *Some privileged users share a password. (Explain below)*
□ *Privileged users with remote access to the system use strong authentication (Explain below)*

The DCS 3000 utilizes a single user class for all ELSUR Operations. All passwords for the accounts on the system are kept on a strict need-to-know basis.

7.3.2.1.3 Device/System User

Account Identifier	Account Privilege Level	Requirement Description
DCSAdmin	Administrator	Runs the DCS 3000 applications.

The DCS 3000 application software requires an account, the DCSAdmin account, with administrative rights in order to operate. The DCSAdmin account must be active in order for the system to operate.

7.3.2.2 Account Management Procedures

7.3.2.2.1 Account Request Procedures

TICTU controls who has knowledge of the system's usernames and passwords on a strict need-to-know basis. TICTU confirms the identity and requirement of any new personnel prior to providing them with the information.

The inherent capabilities of the DCS 3000 operating system are used for password protection. These capabilities are augmented by management mechanisms which provide the following:

- Initial password content and administrative procedures for initial password distribution.
- Length, composition, and generation of passwords.
- Change Processes (periodic and in case of compromise).

- Aging of passwords.
- History of password changes, with assurance of non-replication of individual passwords.
- Protection of passwords to preserve confidentiality and integrity.

7.3.2.2.2 Account Maintenance Procedures

No accounts are modified on the DCS 3000 system. If a user locks out the DCSAdmin account, the ERFAdmin account can be used to unlock the other account.

7.3.2.2.3 Account Termination Procedures

No accounts on the DCS 3000 are ever terminated.

7.3.2.3 Authenticator Procedures

The DCS 3000 employs user IDs and passwords with physical security access requirements to control initial access to the system.

The DCS 3000 uses passwords as its method of user authentication. The system is configured to enforce password complexity as provided by the Windows operating system. All passwords are stored in encrypted form and are changed at least every 90 days. User accounts are disabled for at least 30 minutes after no more than four consecutive unsuccessful attempts are made by the user to supply the correct password.

Upon initial installation of the DCS 3000 system, the SA changes all system-provided administrative default passwords and inserts individualized administrative passwords. With DCS 3000, there are no policies that provide for bypassing user authentication requirements.

Only authorized personnel are allowed into the CMPs where the DCS 3000 systems are located. Each FBI office logs the entry and exit of personnel into the CMPs through an electronic badge system. Individual access to the system can be determined by examining the logs for the electronic badge system for the particular CMP during the time period in question.

7.3.2.3.1 Password Generation

□ *Passwords are generated by the user.*
□ *Passwords generated by the user are validated through the use of automated tools.*
X *Users are encouraged by the ISSO or System Administrator to use “strong passwords” whenever possible*
□ *Users are required to use "strong passwords" generated by the system.*
□ *Passwords are generated by a system (Specify software and provide details below)*

☐ *Passwords are provided by an access control manager (Provide office name below)*

Passwords are randomly generated by the system administrator. These passwords contain at least 8 characters, involve both uppercase and lowercase letters, contain at least one number, and contain at least one special character.

7.3.2.3.2 Password Changes

☐ *Users can change their passwords but are not forced to change their passwords on any timely basis, i.e., passwords are changed whenever the user feels it necessary to change his/her password*

☑ *Users are forced to change their passwords every (Check all that apply):*

☐ *Month* ☐ *Six Months* ☐ *Year*

☐ *NEVER* ☑ *After Initial Login*

☑ *Other:* ***90 Days***

Passwords are stored in encrypted form and are changed at least every 90 days.

7.3.2.4 PKI Use

The DCS 3000 system does not employ PKI.

7.3.3 Accountability (Including Audit Trails)

7.3.3.1 Auditing Procedures

The DCS 3000 provides the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved. The system creates and maintains an audit trail that includes selected records of:

- Successful and unsuccessful logons and logoffs.
- Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.
- Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

The DCS 3000 auditing procedures include individual accountability (i.e., identification of each user and association of that identity with all auditable actions taken by that individual). The DCS 3000 program office will support periodic testing by the ISSO of the security posture of the system, making audit logs available as required to supplement test results.

7.3.3.1.1 Audit Review

Audits or reviews of sensitive applications and re-certification of the adequacy of security safeguards must be performed at least every 3 years.

The purpose of a security evaluation/audit is to identify vulnerabilities, both physical and system-related, and recommend and permanent solutions. A security evaluation/audit is conducted by a disinterested FBI (or other) activity with findings documented in a formal report to be reviewed by the ISSO and SAC of the office audited and by the FBI CIO.

The ISSO reviews audit logs on an as-needed basis.

7.3.3.1.2 Audit Log Storage Requirements

☑ *The audit log is maintained ON-line for*	*Life of the system*
□ *The audit log is maintained OFF-line for*	

Audit logs are maintained on the system for the life of the system. The logs are never deleted or overwritten.

7.3.3.1.3 Discrepancy Handling

Standard FBI procedures in accordance with the FBI Certification and Accreditation Handbook will be invoked when discrepancies are discovered during audit trail reviews.

7.3.3.2 Notification Banner

The following banner is displayed upon logging in to DCS 3000 system:

> This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer system are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

7.3.3.3 User Accountability

□ *The system provides unique identification of each user and association of that identity with all auditable actions taken by that individual*
☑ *The system does NOT provide unique identification of each user and association of that identity with all auditable actions taken by that individual (Explain below)*

The usernames and passwords used in each DCS 3000 system are on a strict need-to-know basis, with few people knowing this information. The identity associated with auditable actions can be determined because so few know the access information. Specific identities can be determined by examining physical security access logs in conjunction with the audit logs. In addition, sites may employ a written log that details who was on a particular system, when the accessed it, and for how long.

7.3.3.4 Audit Protection and Log Access

b2
b7E

7.3.3.4.1 Audit Protection

[redacted]

See section 7.3.3.4.2.

7.3.3.4.2 Audit Log Access

[redacted]

7.3.3.5 Audited Information

7.3.3.5.1 Windows Operating System

☑ *Userid*	☑ *Type of event or action*	☑ *Success or failure of the event*

☑ *Time*	☑ *Terminal or workstation ID*	☑ *System location of the event*
☑ *Date*	☑ *Resources*	☑ *Entity that initiated transaction*
	□ *Remote Access*	☑ *Entity that completed the event*
	Other:	**Other:**

7.3.3.6 Audited Activities

7.3.3.6.1 Windows Operating System

Event Description	Success	Failure	Comment
Logins	☑	☑	
Logoffs	☑	□	
Printing	□	□	
Copying data to removable media	☑	☑	
Use of privileged user or root privileges	☑	☑	
Reading a file or directory	□	□	
Creating a file, directory, or data element(s)	☑	☑	
Deleting a file, directory, or data element(s)	☑	☑	
Attempts to change data	☑	☑	
Use of applications	☑	☑	
Security relevant directories, objects, and incidents	☑	☑	
System console activities	☑	☑	
Information downgrades, and overrides	☑	☑	
Change of user's formal access permissions	☑	☑	

Event Description	Success	Failure	Comment
Attempted access to objects or data whose labels are inconsistent with user privileges	□	□	
Changes to security labels	□	□	
Other: Active Directory Service Access	□	□	

7.3.3.6.2 Other

No other software besides the operating system performs auditing.

7.3.4 System & Communications Protection

7.3.4.1 System Protections

7.3.4.1.1 Malicious Code/Virus Protection

The DCS 3000 workstations are equipped with McAfee VirusScan anti-virus software. This software is updated automatically periodically at regular intervals. The virus definitions are automatically updated via a central server. The latest definitions are obtained from the FBINET and loaded onto this server by a system administrator using "sneakernet" procedures or via remote contro[redacted]

b2
b7E

7.3.4.1.2 Denial of Service Protection

The DCS 3000 system is "closed" in that outsiders cannot gain access to it without defeating multiple layers of physical and electronic security. This multiple-layer approach to information system security is known as "defense-in-depth." Each layer protects the system in a unique way or supplements other layers so a single failure will not compromise the entire system. Since DCS 3000 only receives data from TSPs through controlled and well defined interfaces and does not connect to outside networks, would-be intruders cannot gain access to it electronically by employing known hacking tools and methods.

7.3.4.1.3 Priority Process Protection

Not applicable to the DCS 3000 system.

7.3.4.2 Communications Protection

The DCS 3000 is not connected to any outside system, application, or network other than those proscribed in this document. Furthermore, received data is not re-transmitted externally outside of the CMP. [redacted]nd TSP Proprietary protocols are utilized for all data transmissions into and out of DCS 3000 servers and clients. [redacted] TSP Proprietary, and the PCAnywhere protocols are used to communicate between DCS 3000 components.

b2
b7E

The DCS 3000 uses modems and routers to provide connectivity between the ERF and TSPs. Routers will be configured to use static routing (manually adding routes in each router's routing table) to increase protection by only allowing routing to certain networks.

7.3.4.2.1 Network Allowed Services and Protocols

7.3.4.2.1.1 Internal to the LAN:

SOURCE	DESTINATION	PROTOCOL	SERVICE
Any DCS 3000 Application Component	Any DCS 3000 Application Component	[redacted]	[redacted]
Any DCS 3000 Application Component	Any DCS 3000 Application Component	[redacted]	[redacted]

b2
b7E

7.3.4.2.1.2 External to the LAN:

SOURCE	DESTINATION	PROTOCOL	SERVICE
TSP	DCS 3000	[redacted]	[redacted]
TSP	DCS 3000	[redacted]	[redacted]
DCS 3000	All other external systems listed in section 3.6.1	[redacted]	[redacted]
DCS 3000	All other external systems listed in section 3.6.1	[redacted]	[redacted]

7.3.4.2.2 Controlled Interface Requirements

No firewalls or other controlled interfaces are within the DCS 3000 accreditation boundaries. All firewalls and controlled interfaces noted in this document are described in detail in the accreditations of the other systems. See section 3.6 for more details.

7.3.4.2.2.1 Controlled Interface to DCS 5000

NOMENCLATURE	CONNECTED SYSTEM NAME	PURPOSE
CI100	DCS 5000	Provide one-way pipe to provide call data information to the Secret DCS 5000 (FISA) system.

7.3.4.2.2.2 Controlled Interface to DCS 6000

NOMENCLATURE	CONNECTED SYSTEM NAME	PURPOSE
Cisco Pix	DCS 6000	To control access between the DCS 3000 and the DCS 6000.

7.3.4.3 Unique Security Features

Not applicable to the DCS 3000.

7.3.4.3.1 Mobile/ Executable Code

Not applicable to the DCS 3000 system.

7.3.4.3.2 Collaborative Processing

Not applicable to the DCS 3000 system.

7.3.4.3.3 Distributed Processing

Not applicable to the DCS 3000 system.

7.3.4.3.4 Wireless Devices

Not applicable to the DCS 3000 system.

8. SECURITY AWARENESS PROGRAM

8.1 Program Description

Security awareness training for DCS 3000 personnel focuses on the specific security aspects of the system and integrates hands-on system operations training with systems-specific security considerations and requirements. This "practical training" approach encourages dialogue between trainer and trainee in an operational environment and enhances the learning process as it relates to both system operations and information security. Since these personnel work with the system on a routine basis and have intimate knowledge of its operation and the security considerations related to it, system-specific refresher training is not required.

Beyond this system-specific training, DCS 3000 personnel also receive much broader-based information security training that conforms to the policy and general guidance provided in the FBI MIOG, Part II (Section 35). It is developed and presented by designated FBI security personnel and will be aimed at general users and system administrators. The goals of this training are to:

- Alert FBI personnel to general and specific threats, vulnerabilities, and risks associated with the operation and maintenance of the IT systems they use
- Identify the computer components, data files, etc., that require protection
- Describe the concept of "information accessibility" and how it pertains to the user
- Explain the requirements for information handling, marking, and storage
- Address the physical and environmental aspects of the workplace that users should consider for the protection of their IT systems
- Describe the various types of data and access controls that can be employed with FBI IT systems
- Acquaint the user with contingency plan procedures and what their responsibilities are regarding them
- Explain in general terms what "secure configuration control" means to the average user
- Describe common system security violations and the procedures in place for users to report them
- Ensure users know how to report any inadequacies in FBI Systems Security Training

As part of their newcomers' orientation, new FBI system administrators, operators, and users receive a security awareness briefing within 60 days of their appointment. Continuing security training is provided whenever there is a significant change in FBI information systems security procedures or whenever an employee assumes a new position that requires access to information of greater sensitivity. Refresher training is provided as the SCM deems necessary, and refresher security awareness material is provided to all FBI IT users at least annually. All security training is documented.

8.2 Rules of Behavior

Prior to receiving access to any FBI system, all users are required to review and sign the Rules of Behavior, which was developed by FBI security officials. This document states their security responsibilities as users of the system. By signing this document, the user acknowledges that he or she understands and accepts these responsibilities and will make every effort to comply with them.

The rules of behavior are based upon the principles described in the Computer Security Act of 1987 to protect sensitive information. More specific user responsibilities are set forth in the FBI MIOG and in other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management (OPM) regulations, Office of Management and *Budget (OMB) regulations, and the Standard of Conduct for Federal Employees.* The Rules of Behavior carry the same responsibility for compliance as these official documents. Users who do not comply with these rules are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. The FBI will enforce the use of penalties against any user who willfully violates any DCS 3000 or federal system security (and related) policy.

9. EXCEPTIONS

Not applicable to the DCS 3000 system.

10. GLOSSARY OF TERMS

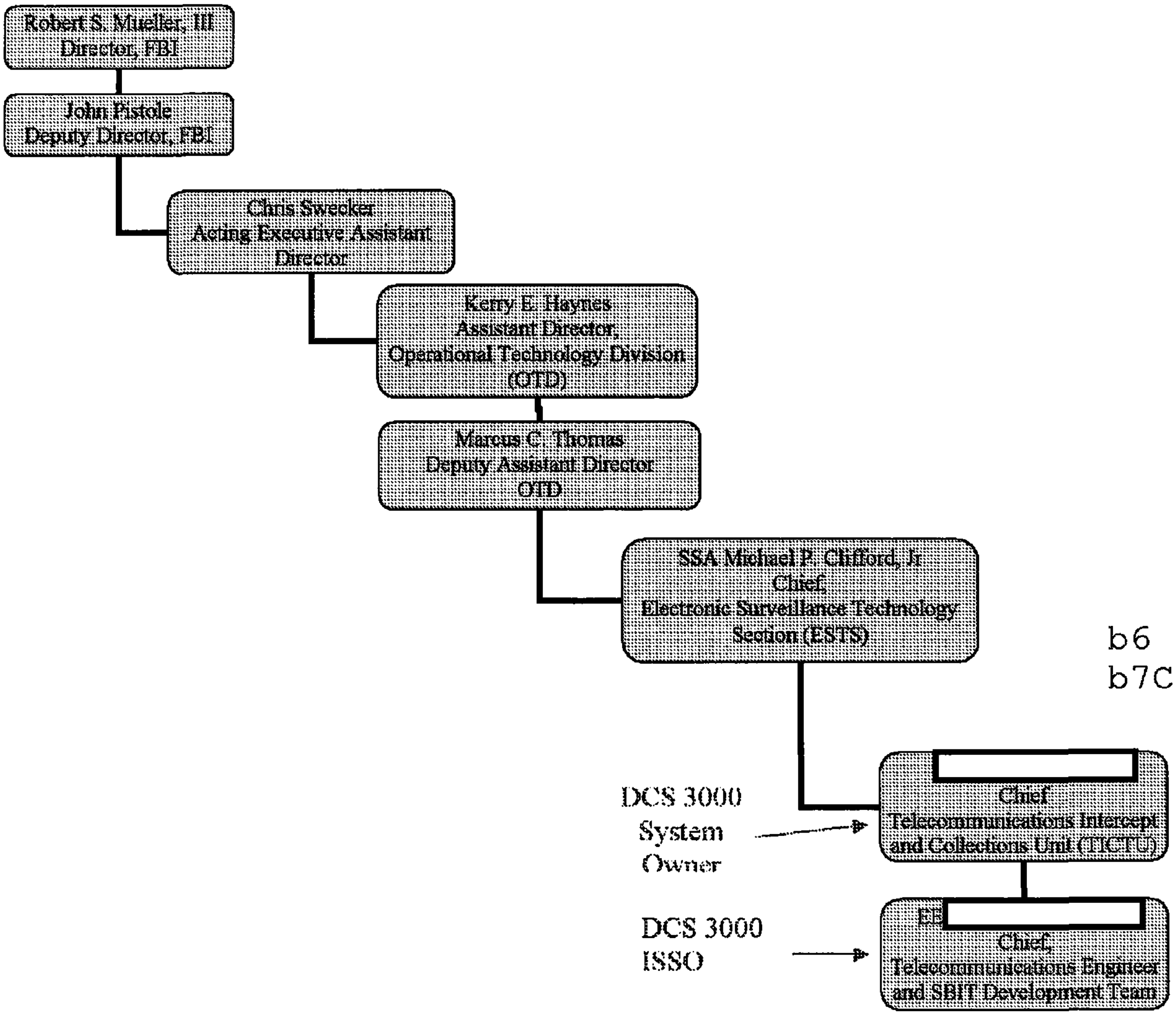
Acronym	Meaning
AES	Advanced Encryption Standard
AIS	Automated Information System (synonymous with IS and IT)
C&A	Certification and Accreditation
CC	Command Criteria
CCTV	Closed Circuit Television
CDC	Call Data Channel
CD	Compact Disc-
CI	Controlled Interface
CI100	Controlled Interface 100
CIO	Chief Information Officer
CLE	Criminal Law Enforcement
CM	Configuration Management
CMCB	Configuration Management Control Board
CMP	Central Monitoring Plant
CONOPS	Concept of Operations
COTS	Commercial-off-the-shelf
DAA	Designated Accrediting Authority
DAC	Discretionary access control
DCID	Direct Central Intelligence, Directive
DCSNET	DCS Network
DOJ	Department of Justice
DOS	Denial of Service
DRP	Disaster Recovery Plan
ELSUR	Electronic Surveillance
ERF	Engineering Research Facility
ESTS	Electronic Surveillance Technology Section
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
GRS	General Records Service
IAS	Information Assurance Section
ID	Identification
IOS	Internetwork Operating System
IP	Internet Protocol
IS	Information System (synonymous with IT and AIS)
ISA	Interconnection Security Agreement
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology (synonymous with AIS and IS)
Kbps	Kilobits per second
KSA	Knowledge, Skills and Abilities

KVM	Keyboard Video Mouse
LAN	Local Area Network
LEA	Law Enforcement Agency
LoC	Level of Concern
MAC	Mandatory Access Control
MAOP	Manual of Administrative Operations and Procedures
Mbps	Megabits per second
MD5	Message Digest Algorithm 5
MIOG	Manual of Investigative Operations and Guidelines
MOA	Memoranda of Agreement
MOU	Memorandum of Understanding
N/A	Not Applicable
NARA	National Archives and Records Administration
O&M	Operations and Maintenance
OTD	Operational Technology Division
PKI	Public Key Infrastructure
PL	Protection Level
PM	Project Manager
PSI	Personnel Security Interview
RA	Risk Assessment
RM	Risk Management
SAC	Special Agent in Charge
SAIC	Senior Special Agent in Charge
SBIT	Switch Based Intercept Team
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SLA	Service Level Agreement
SSP	System Security Plan
SSS	Security Support Structure
TCP	Transmission Control Protocol
TICTU	Telecommunications Intercept and Collection Technology Unit
TSP	Telecommunications Service Provider
TTA	Technically Trained Agent
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network

Attachments

Attachment A - Organizational Structure

See section 1.1.3 for further explanation of the DCS 3000 program organization chart.


Robert S. Mueller, III
Director, FBI
John Pistole
Deputy Director, FBI
Chris Swecker
Acting Executive Assistant Director
Kerry E. Haynes
Assistant Director,
Operational Technology Division (OTD)
Marcus C. Thomas
Deputy Assistant Director
OTD
SSA Michael P. Clifford, Jr
Chief,
Electronic Surveillance Technology Section (ESTS)
DCS 3000
System
Owner
[redacted]
Chief
Telecommunications Intercept and Collections Unit (TICTU)
DCS 3000
ISSO
[redacted]
Chief,
Telecommunications Engineer and SBIT Development Team

b6
b7C

Figure 2: Organization Structure for DCS 3000 Program Management

Attachment B – Detailed System Diagram or System Security Architecture

Connection between the TSP and the FBI is accomplished through a dedicated connection between one TSP and a FBI office. Further explanatory test for the following diagrams is available in Section 3. “System Description.

[redacted]

b2
b7E

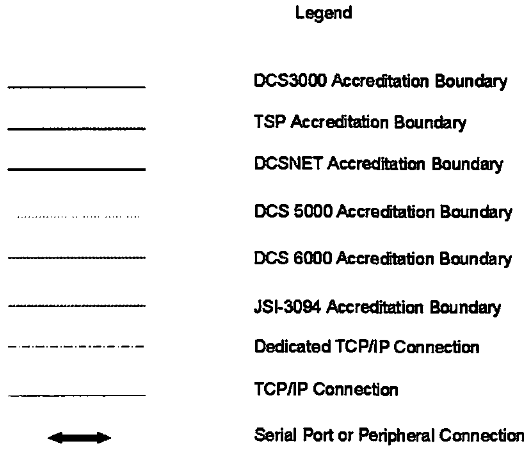

Legend
DCS3000 Accreditation Boundary
TSP Accreditation Boundary
DCSNET Accreditation Boundary
DCS 5000 Accreditation Boundary
DCS 6000 Accreditation Boundary
JSI-3094 Accreditation Boundary
Dedicated TCP/IP Connection
TCP/IP Connection
Serial Port or Peripheral Connection

Figure 3: Typical DCS 3000 Configuration

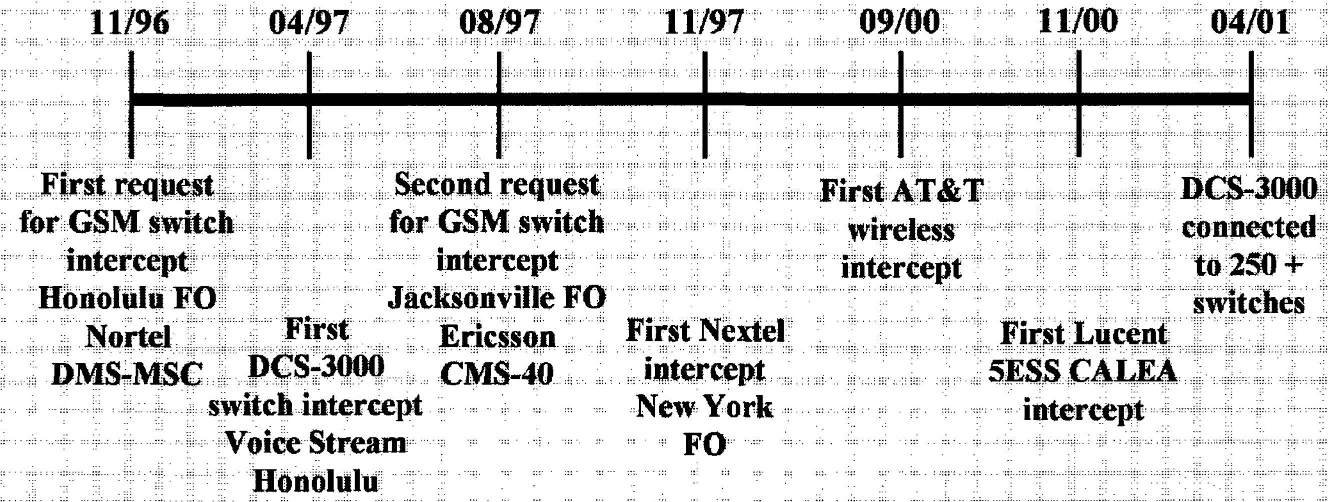
Interim Solutions for Telecommunications Intercepts Course

DCS-3000 As an Interim Solution

DCS-3000

- Initially developed for GSM/PCS-1900 switch intercepts
- FBI's first intercept system for CALEA paradigm
- Windows NT-based Client/Server architecture
  - Windows' ease-of-use
  - Flexibility and scalability

DCS-3000 Timeline



11/96
First request for GSM switch intercept Honolulu FO Nortel DMS-MSC

04/97
First DCS-3000 switch intercept Voice Stream Honolulu

08/97
Second request for GSM switch intercept Jacksonville FO Ericsson CMS-40

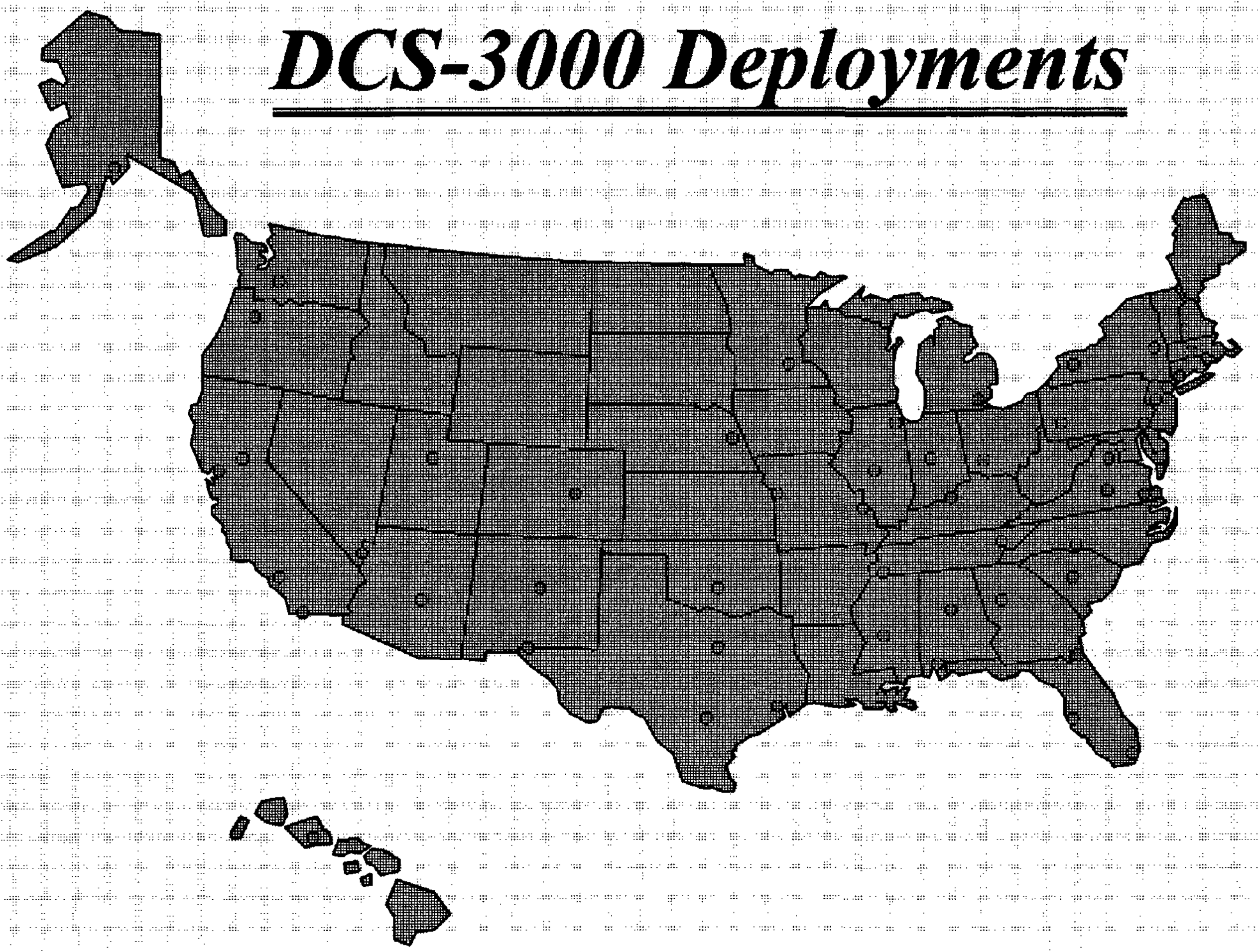
11/97
First Nextel intercept New York FO

09/00
First AT&T wireless intercept

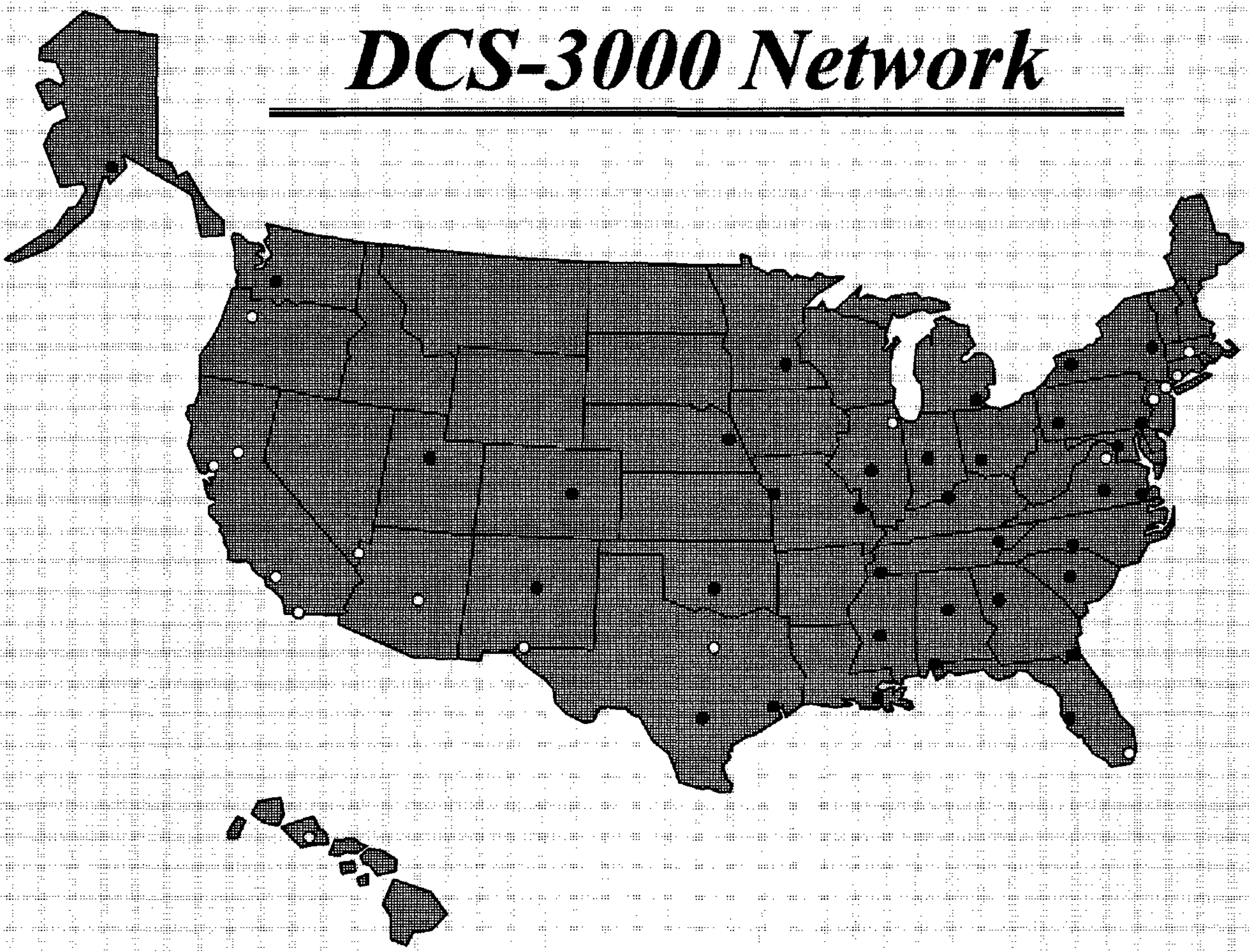
11/00
First Lucent 5ESS CALEA intercept

04/01
DCS-3000 connected to 250 + switches

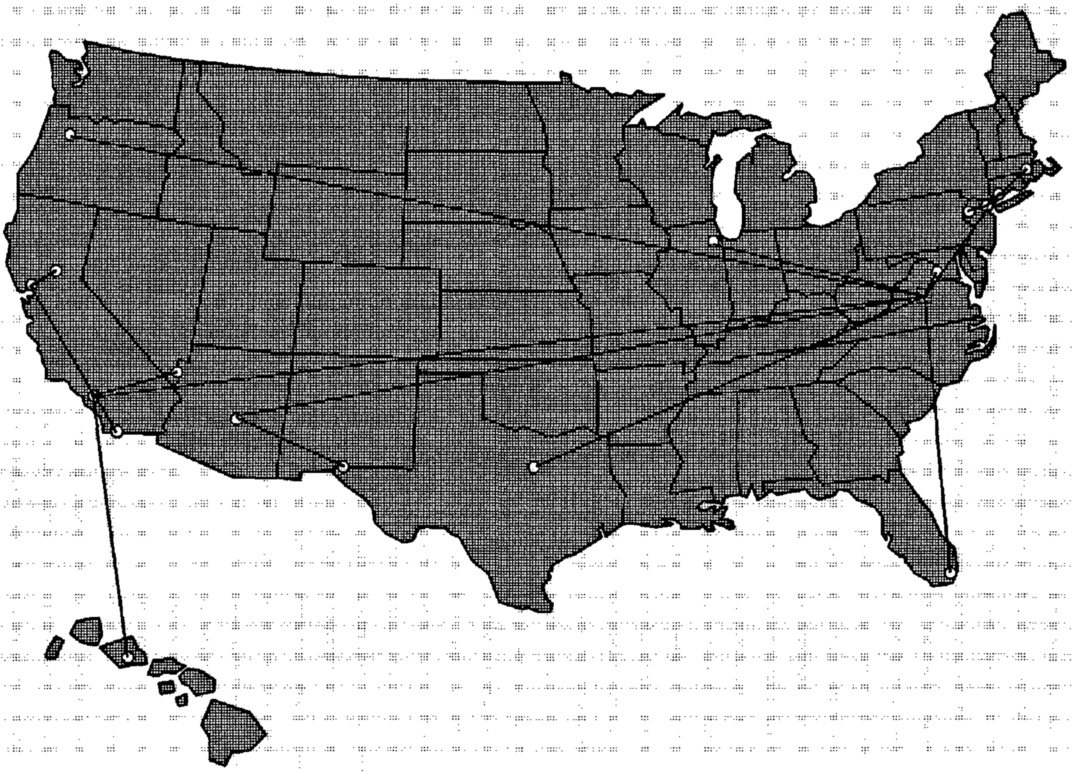
DCS-3000 Deployments



DCS-3000 Network



DCS-3000 Network



DCS-3000

- DCS-3000 is currently deployed in 52 FBI field offices and 250+ switches:

[redacted]

b2
b7E

Switches Intercepted

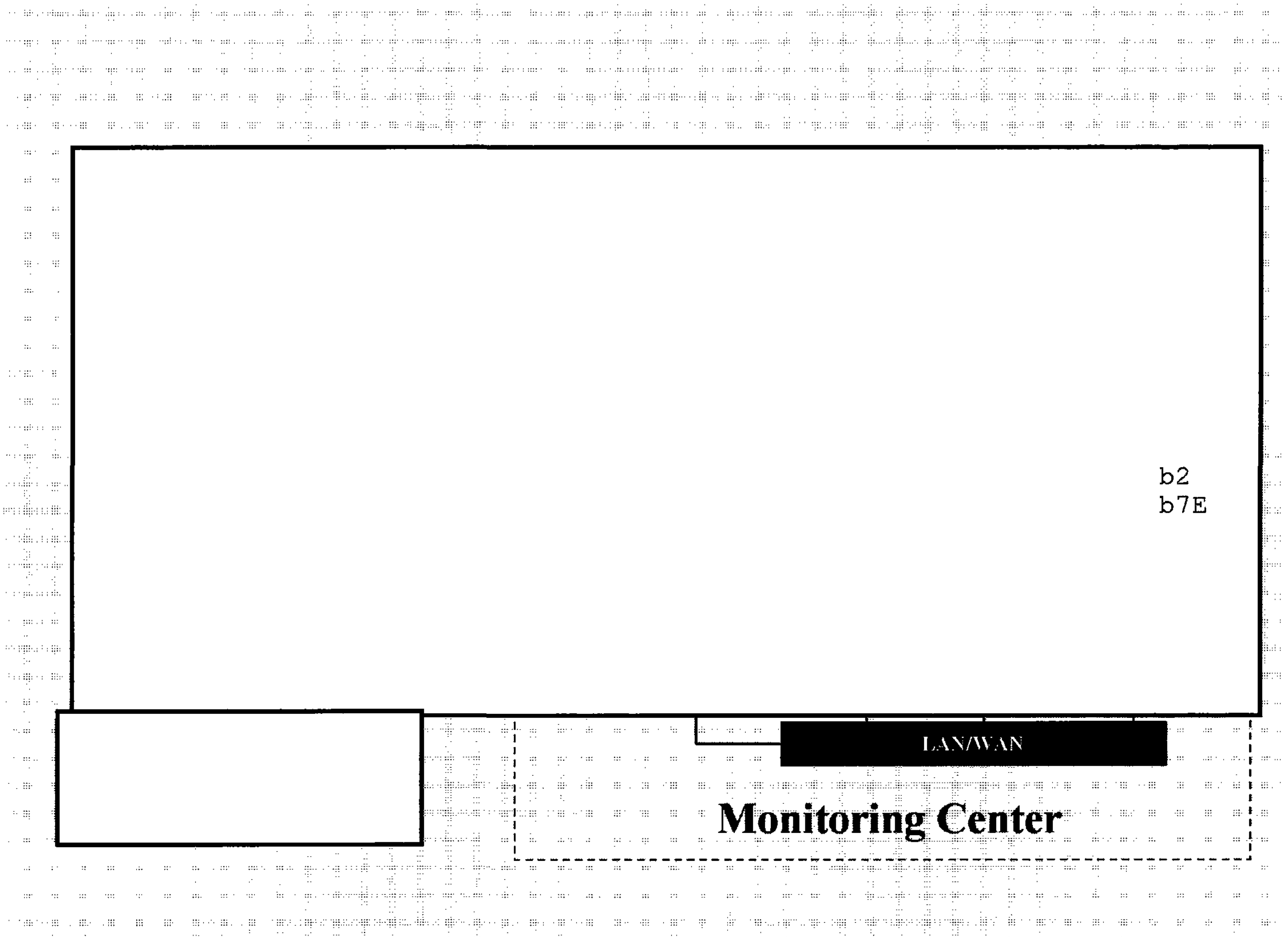
[redacted]

b2
b7E

Single Switch Configuration

[redacted]

b2
b7E



[redacted]

[redacted]

b2
b7E

Questions?