

*Freedom of Information
and
Privacy Acts*

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CD'S

Section: 11



Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 7

- Page 42 ~ Duplicate dupe to pg 1 of Plan of Actions and Milestones
- Page 43 ~ Duplicate dupe to pg 2 of Plan of Actions and Milestones
- Page 44 ~ Duplicate dupe to pg 3 of Plan of Actions and Milestones
- Page 45 ~ Duplicate dupe to pg 4 of Plan of Actions and Milestones
- Page 46 ~ Duplicate dupe to Risk Management Matrix for DCS 300
- Page 47 ~ Duplicate dupe to Risk Management Matrix for DCS 3000 pg 2
- Page 50 ~ Duplicate dupe to pg 2 of Plan of Actions & Milestones

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

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/2/2006

To: Operational Technology

Attn: [redacted]

Security

Attn: [redacted]

b6
b7C

From: Security

Information Assurance/Accreditation/SPY-B F-501

Contact: [redacted] 202-[redacted]

Approved By:

[redacted] *lms as/yp/ps*

Drafted By:

[redacted] mlm

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

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

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

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

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

The Levels of Concern (LoC) are Medium for Confidentiality, Medium for Integrity, and Medium for Availability. DCS-3000 is a Sensitive but Unclassified (SBU) system operating in the System High Mode of Operation. The

To: Operational Technology From: Security
Re: 319U-MQ-1487677-SECD, 05/2/2006

DCS-3000 has been assessed as a Tier Level 2 in accordance with the FBI Certification and Accreditation Handbook.

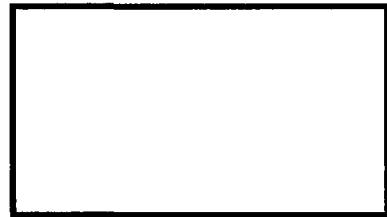
b2
b7E

The DCS-3000 application suite was developed to assist Law Enforcement Agencies (LEA) with collecting and processing data for court-ordered Electronic Surveillance (EUSUR) operations. The DCS-3000 collects [REDACTED]

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

The Certification and Accreditation Team Members are:

System Owner:
Information System Security Officer:
System Administrator:
Information System Security Manager:
Certification Representative:
Accreditation Representative:



b6
b7C

To: Operational Technology From: Security
Re: 319U-HQ-1487677-SECD, 05/2/2006

LEAD(s):

Set Lead 1: (Info)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

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

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

For information only.

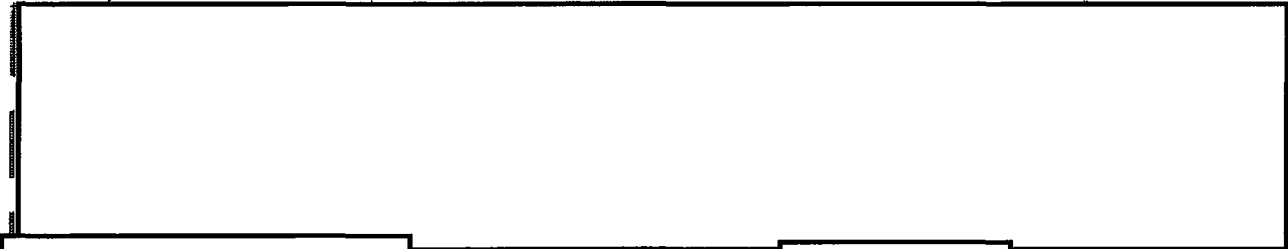
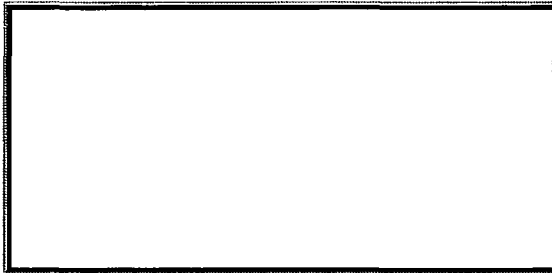
CC:



b6
b7C

◆◆

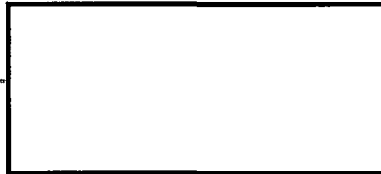
DCS-3000 Accreditation Diagram



DCS-3000 Accreditation
Boundary



b2
b7E



DCS-5000



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/01/2006

To: Operational Technology

Attn:

Security

Attn:

From: Security

Information Assurance/Accreditation/SPY-B F-501

Contact: [Redacted] 202-[Redacted]

b6
b7C

Approved By:

[Redacted] *IAS 06/01/06*

Drafted By:

[Redacted] :mjm

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

Serial 300

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

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

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

Administrative: References:

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

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

To: Operational Technology From: Security
Re: 319U-HQ-A1487677-SECD, 06/01/2006

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

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

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

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

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

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

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

1. A full security assessment be completed within 180 days to ensure appropriate security controls have been implemented that address changes in the architecture that have occurred.
2. All vulnerabilities be successfully resolved or mitigated within the 180 day period.

To: Operational Technology From: Security
Re: 319U-HQ-A1487677-SECD, 06/01/2006

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

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

To: Operational Technology From: Security
Re: 319U-HQ-A1487677-SECD, 06/01/2006

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

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

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

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

CC:



b6
b7C

◆◆



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

June 1, 2006

Mr. Vance E. Hitch
Chief Information Officer
U.S. Department of Justice
Room 1310
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Hitch:

The purpose of this communication is to notify the Department of Justice (DOJ) of the Approval to Operate (ATO) for the Digital Collection System - 3000 (DCS-3000). This ATO has been issued by the FBI's Designated Accrediting Authority (DAA) for a period of three years from 06/01/2006 to 06/01/2009.

The DAA Representative, in conjunction with the System Certification Team, have determined the Levels of Concern (LOC) assigned for DCS-3000 are Medium for Confidentiality, Medium for Integrity and Medium for Availability. DCS-3000 has been assessed as a Tier Level 2 system in accordance with the FBI Certification and Accreditation Handbook.

Sincerely yours,

*DCS-3000 IS ATO
3/11/06 11:48 AM
S. J. [unclear]*

[Redacted] on behalf of
Saimal Azmi
Chief Information Officer
Designated Accrediting Authority

b6
b7c

*3/11/06 11:48 AM - Serial # 300
S. J. [unclear]*

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/VE

**DCS 3000J System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]**

Page/Section/Paragraph	Title	SRTM #	Pass/Fail	Comments
	Table of Contents			
	Introduction			
1	Information System General Information			
1.1	Security Administration			
1.1.1	System Information			
1.1.2	Key System Points of Contact			
1.1.3	Security Organization			
1.2	Mission			
1.2.1	Purpose and Scope			
1.2.2	Supported Projects			
1.2.3	Information System Usage			
1.3	Inter-Departmental/Agency Use and Agreements			
1.3.1	Joint Use Information			
1.3.2	Memorandum of Agreement (MOA)/Understanding (MOU)			
1.3.3	Interconnection Security Agreement (ISA)			
2	Secure Facility Description			
2.1	Facility Layout			
2.2	Physical and Environmental Protection			
2.2.1	Physical Protection			

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

DCS 3000J System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
2.2.2	Environmental Protection			b2 b7E
2.3	System Layout			
2.4	Emanation Protection			
2.4.1	Red/Black Separation			
2.4.2	TEMPEST			
3	System Description			
3.1	Summary			
3.2	Protection Level/Mode of Operatio			
3.3	Levels of Concern			
3.3.1	Confidentiality			
3.3.2	Integrity			
3.3.3	Availability			
3.4	Tier Designation			
3.5	System Diagram			
3.6	Interconnection Interface Description			
3.6.1	Direct Network Connection			
3.6.1.1	Connectivity Management Procedures			
3.6.1.2	Interconnection			
3.6.1.3	Connectivity Procedures			
3.6.1.4	Networking			
3.6.2	Indirect Connections			
3.6.2.1	Indirect Import			

DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
3.6.2.2	Indirect Export			
3.7	Data Processed			
3.7.1	Classification and Compartments			
3.7.2	Dissemination Controls			
3.7.3	Type of Data Processed			
3.8	Data Flow Diagram			
4	System Hardware			
4.1	Hardware List			
4.2.1	Labeling of System Hardware			
4.2.2	(System Hardware) Exceptions			
4.3	Sanitization and Destruction			
4.4	Custom-Built Hardware			
5	System Software			
5.1	Software List			
5.2	Software with Restricted Access or Limited Use Requirements			b2 b7E
5.3	Foreign Software			
5.4	Freeware/Shareware/Open-Source Software			
5.5	(System Software) Marking and Labeling			
6	Data Storage Media			
6.1	Media Type			
6.2	Media Handling			
6.2.1	Media Introduction and Removal			

DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section #/Paragraph	Title	SRTM #	Pass/Fail	Comments
6.2.2	Sanitization and Destruction			
6.3	Storage Media Marking and Labeling			
7	Security Control Requirements			
7.7.1	Risk Assessment			
7.1.2	Compliance and Monitoring Program			b2 b7E
7.2.1	Personnel Security			
7.2.1.1	Non-US Citizens			
7.2.2	Contingency Planning			
7.2.2.1	System Backup			
7.2.2.1.1	Backup Protection			
7.2.2.1.2	On-site & Off-site Storage			
7.2.2.2	Telecommunications Services			
7.2.2.3	Backup Power Supply Requirements			
7.2.2.4	Recovery Procedures			
7.2.2.4.1	Continuity of Operations Plan			
7.2.2.4.2	Disaster Recovery Plan			
7.2.3	Configuration Management Program			
7.2.3.1	Hardware & Software Procurement			
7.2.3.2	Evaluation			

DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
7.2.4	Maintenance			
7.2.4.1	Maintenance and Repair Procedures			
7.2.4.2	Maintenance Procedures Using Uncleared Personnel			
7.2.4.3	Maintenance Logs			
7.2.4.4	Hardware & Software Maintenance			
7.2.4.4.1	System Start-Up/Shut-Down			
7.2.4.4.2	Security Controls and Operations During Maintenance			
7.2.4.4.3	Remote Diagnostics			
7.2.4.4.4	Hardware & Software Transfer, Relocation, and Release			
7.2.5	System & Information Integrity			
7.2.5.1	System Integrity			
7.2.5.1.1	System Start-up			
7.2.5.1.2	After Hours Processing Procedures			
7.2.5.2	Data and Software Integrity			
7.2.5.2.1	Data and Software Integrity Procedures			
7.2.5.2.2	Data Copying, Reviewing, and Release Procedures			b2 b7E
7.2.5.2.3	Printout/Hardcopy			
7.2.5.2.4	Non-Repudiation			
7.2.5.2.5	Transaction Rollback			
7.2.6	User's Guides			
7.2.6.1	Configuration Guides			
7.2.6.2	Guides for Privileged Users			

**DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]**

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
7.2.6.3	Guides for General Users			
7.2.7	Incident Response			
7.2.7.1	ISSO Notification during Suspicious Events			
7.2.7.2	Actions Taken By System During Suspicious Events			
7.3	Technical			
7.3.1	Access Control			
7.3.1.1	Discretionary Access Control (DAC)			
7.3.1.1.1	Need-To-Know Controls			b2 b7E
7.3.1.1.2	Discretionary Access Control Augmentation			
7.3.1.2	Mandatory Access Controls (MAC)			
7.3.1.2.1	Internal Marking and Labeling			
7.3.1.3	Technical Access Control Mechanism			
7.3.1.4	User Group and Access Rights			
7.3.1.4.1	User Groups			

**DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]**

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
7.3.1.4.1.1	Privileged User Group Roles			
7.3.1.4.1.2	General User Group Roles			
7.3.1.4.2	System Access Rights			
7.3.1.4.2.1	Local System Access Rights			
7.3.1.4.2.2	Remote System Access			b2
7.3.1.4.2.3	Non-Data File Access			b7E
7.3.1.4.3	Privileged Users Access Rights			
7.3.1.5.1	Log-On Error Handling			
7.3.1.5.1	Log-on Error Handling			
7.3.1.5.2	Account Lockout Handling			
7.3.2	Identification & Authentication			
7.3.2.1	System Users			
7.3.2.1.1	General Users			
7.3.2.1.2	Privileged User			
7.3.2.1.3	Device/System User			
7.3.2.2	Account Management Procedures			
7.3.2.2.1	Account Request Procedures			
7.3.2.2.2	Account Maintenance Procedures			
7.3.2.2.3	Account Termination Procedures			
7.3.2.3	Authenticator Procedures			
7.3.2.3.1	Password Generation			
7.3.2.3.2	Password Changes			
7.3.2.4	PKI Use			
7.3.2.5	Trusted Multi-Level Communication Path			
7.3.3	Accountability (Including Audit			

**DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]**

Page/Section Paragraph	Title	SRTM #	Pass/Fail	Comments
	Trails)			
7.3.3.1	Auditing Procedures			
7.3.3.1.1	Audit Review			b2
7.3.3.1.2	Audit Log Storage Requirements			b7E
7.3.3.1.3	Discrepancy Handling			
7.3.3.1.4	System Shutdown During Audit Failure			
7.3.3.2	Notification Banner			
7.3.3.3	User Accountability			
7.3.3.4	Audit Protection and Log Access			
7.3.3.4.1	Audit Protection			
7.3.3.4.2	Audit Log Access			
7.3.3.5	Audited Information			
7.3.3.5.1	Windows Operating System			
7.3.3.5.2	Solaris Operating System			
7.3.3.5.3	Oracle Database			
7.3.3.5.4	Microsoft SQL Database			
7.3.3.5.5	Microsoft Internet Information Server (IIS)			
7.3.3.6	Audited Activities			
7.3.3.6.1	(Audited Activities) Windows Operating System			
7.3.3.6.2	(Audited Activities) Solaris Operating System			
7.3.3.6.3	(Audited Activities) Oracle Database			
7.3.3.6.4	(Audited Activities) Microsoft SQL Database			

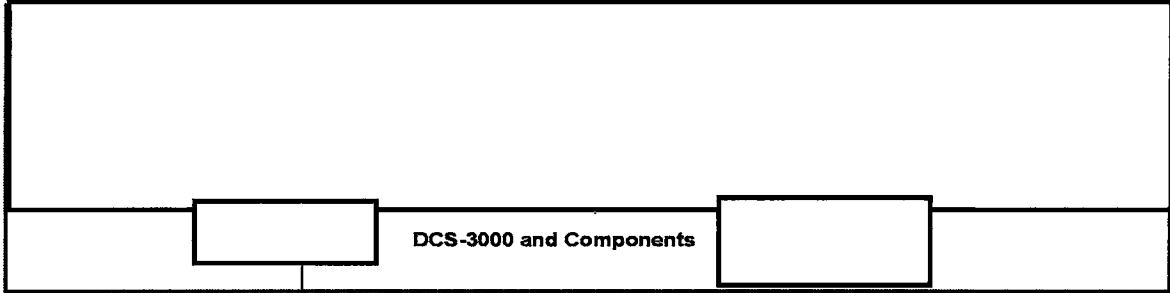
DCS 3000J System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section /Paragraph	Title	SRTM #	Pass/Fail	Comments
7.3.4	System & Communications Protection			
7.3.4.1	Systems Protections			
7.3.4.1.1	Malicious Code/Virus Protection			
7.3.4.1.2	Denial of Service Protection			
7.3.4.1.3	Priority Process Protection			
7.3.4.2	Communications Protection			
7.3.4.2.1	Network Allowed Services and Protocols			
7.3.4.2.1.1	Internal to the LAN:			
7.3.4.2.1.2	External to the LAN:			b2
7.3.4.2.2	Controlled Interface Requirements			b7E
7.3.4.2.2.1	Controlled Interface to System #1			
7.3.4.2.2.2	Controlled Interface to System #2			
7.3.4.3	Unique Security Features			
7.3.4.3.1	Mobile/Executable Code			
7.3.4.3.2	Collaborative Processing			
7.3.4.3.3	Distributed Processing			
7.3.4.3.4	Wireless Devices			
8.1	(Security Awareness Program) Program Description			

DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section/Paragraph	Title	SRTM #	Pass/Fail	Comments
8.2	Rules of Behavior	[REDACTED]		
9	Exceptions			
10	Glossary			
ATTACHMENTS				
A	Organizational Structure	[REDACTED]		
B	Detailed System Diagram or System Security Architecture			
C	Facility Layout and Overview or System Equipment Location Floor Plan			Multiple floor plan system deployed to 80 cites
D	Equipment List			b2
E	Software List			b7E
F	Agreements (MOA, MOU, ISA)			
G	Training Materials			
H	System Requirements			
I	Testing Plans and Results			
J	Risk Management Matrix (RMM)			
K	Certification EC			
L	Accreditation Risk Management Report (RMP)			
M	Accreditation EC			
N	Accreditation Letter to DOJ			
O	Configuration Management Plan (CMP)			
P	Privileged & General Users Guides			
Q	Contingency Plan (CP)			
R	Disaster Recovery Plan (DRP)			

b2
b7E



DCS-3000 and Components



DCS-3000 Accreditation Boundary

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/28/2003

To: Investigative Technology

Attn:



From: Security

IAS/AU/4282

Contact:



(202) 324



b6
b7C

Approved By: Hooton William L



Drafted By:



mgm

Case ID #: 66F-HQ-A1403623-J Serial #93

Title: ACCREDITATIONS

NOTIFICATION OF ACCREDITATION DECISION FOR THE DATA
COLLECTION SYSTEM 3000 (DCS3000)

Synopsis: To notify the system owner of the Data Collection System 3000 (DCS3000) accreditation and address an outstanding action item.

Reference: 66F-HQ-C1333650-DCS3000

Details: The Security Division's Accreditation Unit (AU) has completed the requested review of the System Security Plan (SSP) and the Risk Report dated December 17, 2002 and received March 25, 2003. Resulting from this review, the Designated Accrediting Authority (DAA) has accredited the DCS3000 from May 28, 2003 through May 27, 2006.

The DCS3000 was assessed as a Tier 2 system with Confidentiality - High, Integrity - High and Availability - Medium. The system is accredited to operate at the SBU level, Dedicated Security Mode of Operation.

The DCS3000 accreditation is contingent upon developing and implementing audit retention and review procedures within 180 days. The Information Technology Security Unit (ITSU) will provide verification to the AU of audit retention and review procedures within this time frame. Maintaining a current accreditation status is subject to completing this action as well as to the continued

To: Investigative Technology From: Security
Re: 66F-HQ-A1403623-J, 05/28/2003

adherence to the provisions of the SSP. In particular, all media copied or downloaded from the DCS3000 must be scanned for malicious code with the latest available virus scan updates before introducing information to any application residing on FBINET.

To: Investigative Technology From: Security
Re: 66F-HQ-A1403623-J, 05/28/2003

LEAD(s) :

Set Lead 1: (Action)

INVESTIGATIVE TECHNOLOGY

AT WASHINGTON, DC

Develop and implement audit retention and review procedures within 180 days.

CC -



◆◆

b6
b7C



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

May 28, 2003

Mr. D. Jerry Rubino
Department Security Officer
U.S. Department of Justice
RFK Building
Room 6525
Washington, D.C., 20530

Dear Mr. Rubino:

The purpose of this communication is to notify DOJ of the Data Collection System 3000 (DCS3000) accreditation.

The system is accredited to operate at the SBU level, Dedicated Security Mode of Operation. It was assessed as a Tier 2 system with Confidentiality - High, Integrity - High and Availability - Medium.

An exception to DOJ policy is requested, as an exception to FBI policy requiring a user account to be unlocked by a system administrator after three unsuccessful attempts has been granted. The mitigating strategy described in the SSP fulfills the intent of FBI and DOJ policies.

The Security Division's Accreditation Unit conducted the DCS3000 accreditation in accordance with the requirements set forth in Bureau, Departmental, and National policy. Accreditation is granted for a period of three years or until major changes affecting the security profile of the system are made. The accreditation period is from May 28, 2003 and will expire May 27, 2006.

Sincerely,

William L. Hooton
Deputy Executive
Assistant Director
Administration

Enclosure

Case ID # 66F-HQ-A1403623-J Serial# 91



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

b6
b7C

May 28, 2003

[REDACTED]
Federal Bureau of Investigation
Room 9396
Washington, D.C. 20535

Dear [REDACTED]

The purpose of this communication is to accredit the Data Collection System 3000 (DCS3000). The Security Division's Accreditation Unit has completed the requested review of the System Security Plan (SSP), dated December 17, 2002 and received March 25, 2003.

The system is certified to operate at the SBU level, Dedicated mode of operation. It was assessed by the certifier as a Tier 1, Protection Level 1 system with Confidentiality - Medium, Integrity - Medium and Availability - Medium.

The Security Division's Accreditation Unit conducted the DCS3000 accreditation in accordance with the requirements set forth in Bureau, Departmental, and National policy. Accreditation is granted for a period of three years or until major changes affecting the security profile of the system are made. The accreditation period is from May 28, 2003 and will expire May 27, 2006.

**ACCREDITATION STATEMENT FOR THE
DATA COLLECTION SYSTEM 3000 (DCS3000)**

Sincerely,

William L. Hooton
Executive Assistant Director

Case ID # 66F-HQ-A1403623-J Serial# 94



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 1, 2006

Mr. Vance E. Hitch
Chief Information Officer
U.S. Department of Justice
Room 1310
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Hitch:

The purpose of this communication is to notify the Department of Justice (DOJ) of the Approval to Operate (ATO) for the Digital Collection System - 3000 (DCS-3000). This ATO has been issued by the FBI's Designated Accrediting Authority (DAA) for a period of three years from 06/01/2006 to 06/01/2009.

The DAA Representative, in conjunction with the System Certification Team, have determined the Levels of Concern (LoC) assigned for DCS-3000 are Medium for Confidentiality, Medium for Integrity and Medium for Availability. DCS-3000 has been assessed as a Tier Level 2 system in accordance with the FBI Certification and Accreditation Handbook.

Sincerely yours,

on behalf of
Zaimal Azmi
Chief Information Officer
Designated Accrediting Authority

b6
b7C

319U-HQ-A1487677-SECD Serial # 306

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

FOR OFFICIAL USE ONLY



Data Collection System 3000 (DCS-3000)

Plan Of Actions & Milestones (POA&M)

June 1, 2006

Version 1.0

Prepared by:

b6
b7C

Quantico ISSM



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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

1. INTRODUCTION

1.1. System Description

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

[REDACTED]

- [REDACTED]

b2
b7E

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

- [REDACTED]

- [REDACTED]

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

b2
b7E

The DCS-3000 system is deployed in central monitoring plants (CMP) [REDACTED]

[REDACTED] is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).

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

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

2. RISK ASSESSMENT RESULTS

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

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

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

2.1. Risk Assessment

2.1.1. High Risk Vulnerability/Threat Pairs

The following are the remaining high-risk vulnerability/threat pairs that are drawn from the initial RMM table. There are seven operational aspects of this collection system that appear to be at high risk. Overarching mitigating factors for these risks include the DCS-3000 working environment at each operating location (i.e. [redacted])

[redacted]

operations and must undergo a thorough and comprehensive screening process in order to be granted an FBI Top Secret clearance before being authorized to perform their tasks.

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

[redacted]

Current Status:

- [redacted]

[redacted]

Current Status:

[redacted]

b2
b7E

FOR OFFICIAL USE ONLY

[Redacted]

Current Status:

[Redacted]

[Redacted]

[Redacted]

b2
b7E

Current Status:

- [Redacted]

Planned or Recommended Remedial Action:

[Redacted]

[Redacted]

[Redacted]

Current Status:

- [Redacted]

[Redacted]

[Redacted]

b2
b7E

Current Status:

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

[Redacted]

Current Status:

[Redacted]

2.1.2. Medium Risk Vulnerability/Threat Pairs

[Redacted]

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

[Redacted]

Current Status:

- [Redacted]

b2
b7E

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

RISK MANAGEMENT MATRIX FOR DCS-3000

Risk Analysis		Risk Management	
Identify Risk	Significance of Scenario Risk to ASW/ASW-C3000	Mitigation/Recommended Controls/Process Result/Residual Risk	
		b2 b7E	

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

RISK MANAGEMENT MATRIX FOR DCS-3000

Risk Analysis		Risk Management			
Vulnerability (V)	Issue (I) Analyzed	Significant (S) or Occurrence (O)	Risk to Assets (R)	Mitigation (M) Recommended	Control Measures (C) Implemented (N/A) (M)

b2
b7E

FOR OFFICIAL USE ONLY

Concerns

(U) There are several areas of the total DCS-3000 program that require additional correction/improvement. Because the final engineering of the system is not completed, and the former certification testing was accomplished approximately four years ago, a full system test is required once the system architecture has achieved stasis. In addition, the DCS-3000 SSP [redacted]

[redacted]

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

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

b2
b7E

Conclusion

(U) The DCS-3000 has very few existing vulnerabilities, and is an SBU system. [redacted]

[redacted]

[redacted]

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

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

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/28/2003

To: Director's Office

Attn: William L. Hooton

From: Security

IAS/AU/4282

Contact: [redacted] (202) 324 [redacted]

Approved By: [redacted]

b6
b7C

Drafted By: [redacted] mgm

Case ID #: 66F-HQ-A1403623-J **Serial #92**

Title: ACCREDITATIONS - REQUEST FOR ACCREDITATION DECISION FOR THE DATA COLLECTION SYSTEM 3000 (DCS3000)

Synopsis: To request an accreditation decision by the DAA for the Data Collection System 3000 (DCS3000).

b2
b7E

Reference: 66F-HQ-C1333650-DCS3000

Details: The Data Collection System 3000 (DCS3000) was assessed as a Tier 2 system with Confidentiality - High, Integrity - High and Availability - Medium. The system is certified to operate at the SBU level, Dedicated Security Mode of Operation.

The DCS3000 is an electronic surveillance (ELSUR) collection system that supports criminal law enforcement (CLE) Title III criminal investigations. The DCS3000 application suite resides on a [redacted]

[redacted] The completion of actions detailed in an EC from Security, Case ID #66F-HQ-A1403623-J, to Investigative Technology dated 05/28/2003 will minimize the risk to FBINET.

The Security Division's Accreditation Unit conducted the DCS3000 accreditation review in accordance with the requirements set forth in Bureau, Departmental and National policy. Favorable approval by the DAA will accredit the DCS3000 for a period of three years or until major changes affecting the security profile of the system are made. The accreditation period is from May 28, 2003 and will expire May 27, 2006.

To: Director's Office From: Security
Re: 66F-HQ-A1403623-J, 05/28/2003

LEAD(s) :

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT EADADMIN, DC

Request an accreditation decision for the Data
Collection System 3000 (DCS3000).

◆◆

FOR OFFICIAL USE ONLY



Data Collection System 3000 (DCS-3000)

System Security Plan Risk Management Matrix (RMM)

June 1, 2006

Version 2.0

**Prepared by
Information Assurance Section/Accreditation Unit
(IAS/AU)
SPY-B Room 501**

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

FOR OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY



DCS3000
Systems Security Plan
Appendix C
Risk Management Matrix (RMM)

November 5, 2002
Version 1.0 – November 5, 2002

b6
b7C

Prepared For:

[Redacted]
[Redacted] *Legacy System Certification Unit (LSCU)*
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Room 1302
Washington, DC 20530

Prepared By:

LSCU [Redacted]
FBIHQ

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65279 DMH/TAM/KSR/JB

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

1. INTRODUCTION

1.1. System Description

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

[REDACTED]

[REDACTED]

b2
b7E

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

[REDACTED]

[REDACTED]

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

b2
b7E

The DCS3000 system is deployed in central monitoring plants (CMP) [REDACTED]

[REDACTED] is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).

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

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

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

LIMITED OFFICIAL USE ONLY

[Redacted]

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

[Redacted]

b2
b7E

Planned or Recommended Remedial Action:

[Redacted]

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

LIMITED OFFICIAL USE ONLY

2.1.2 Medium Risk Vulnerability/Threat Pairs

[Redacted]

Planned or Recommended Remedial Action:

[Redacted]

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

b2
b7E

RISK MANAGEMENT MATRIX FOR DCS3000

Risk Analysis		Risk Management	
What? (What)	How? (How)	Why? (Why)	When? (When)

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

(1)

RISK MANAGEMENT MATRIX FOR DCS3000

Risk Analysis					Risk Management		
Severity (V)	Probability (A)	Significance (S)	Control (C)	Risk to Assets (R)	Mitigation Recommended	Control Status	Resulting Risk (R)

--	--	--	--	--	--	--	--

b2
b7E

**RISK MANAGEMENT PLAN
(RMP)**

FOR THE

**Data Collection System – 3000
(DCS-3000)**



Prepared by

June, 01, 2006

**Prepared by
Information Assurance Section/Accreditation Unit
(IAS/AU)
SPY-B Room 501**

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB



Table of Contents

1. Purpose of the Risk Management Plan..... 3
2. Mission/Description of the DCS-3000..... 3
3. Security Characteristics and Accreditation Boundary.... 3
4. Decision Issues for the DCS-3000..... 3
5. Recommendation..... 4

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

1. Purpose of the Risk Management Plan

The Risk Management Plan (RMP) provides the Designated Accrediting Authority (DAA) and other FBI executives the general essential elements of information relative to the Data Collections System (DCS-3000) to include the strategy to address the identified vulnerabilities.

b2
b7E

2. Mission/Description of the DCS-3000

The DCS-3000 system is deployed in central monitoring plants (CMP) [redacted]
[redacted]
[redacted] is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).
FBI professionals, who have been well screened, cleared, and trained for the operations they perform, operate and use the system in a physically secure, climate-controlled environment. The system is easy to use, and personnel duties are clearly defined and appear to be commonly understood so stress levels for system users, regardless of their positions, are fairly low, especially in light of the types of work they do.

3. Security Characteristics and Accreditation Boundary

The DCS-3000 is operating at the Sensitive but Unclassified (SBU) level in the System High mode of operation. The system has been designated as Tier [redacted] system that operates at a [redacted] Level of Concern (LOC) for [redacted] Integrity, and Availability.

b2
b7E

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

4. Decision Issues for the DCS-3000

The following table summarizes the vulnerabilities and accepted risks for DCS-3000:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

DCS-3000 Risk Evaluation

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b2
b7E

LIMITED OFFICIAL USE ONLY



DCS3000
System Rules of Behavior
APPENDIX D

March 13, 2003

Prepared For:

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

b6
b7C

Prepared By:
The LSCU Green Team
FBIHQ

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	Purpose.....	1
1.1.2	User Information and Contacts	1
1.1.3	The DCS3000 Environment	3
1.2	Interacting With Administrators.....	4
1.3	Configuration Management.....	5
1.3.1	Things You May Change.....	5
1.3.2	Things You May Not Change.....	5
1.4	Unauthorized Activities	6
1.5	Your Role In Protecting the System.....	7
2.0	USER SUPERVISORS.....	8
2.1	Account Creation Responsibilities	8
2.2	Account Termination Responsibilities	8
2.3	Account Parameters.....	8
2.4	Account Verification/Validation	9
2.5	Awareness Responsibilities.....	9
2.6	Official Use.....	9
2.7	Incident Reporting.....	9
3.0	ADMINISTRATORS.....	9
3.1	System Administrators.....	9
3.1.1	Responsibilities.....	9
3.1.2	Separation of Duties.....	10
3.2	ISSO.....	10
4.0	INFORMATION SYSTEMS SECURITY MONITORING.....	11
5.0	MONITORING NOTICES.....	11
5.1	Computer Log-on Banner.....	12
6.0	SYSTEM ADMINISTRATORS	12
6.1	Objective.....	12
6.2	Restrictions on System Administrators in the Normal Performance of Their Duties	13
6.3	Management Searches	14
6.4	Assistance To Law Enforcement And Counterintelligence	14

LIMITED OFFICIAL USE ONLY

1.0 INTRODUCTION

Prior to receiving access to DCS3000, all users shall be required to review the DCS3000 Rules of Behavior. These Rules of Behavior apply to all users of DCS3000. 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. Copies of these rules of behavior must be provided to all new users of DCS3000 before they are granted system access.

Security is important for everyone. All users of DCS3000 resources should be aware that the system as a whole contains valuable and sometimes sensitive government information, which must be protected to prevent disclosure, unauthorized changes, and loss. Each part of the system can introduce vulnerabilities to the whole, so protection must be consistent in order to be effective.

1.1 Purpose

The purpose of the DCS3000 Rules of Behavior is to implement baseline security requirements for all program managers (PM), system administrators (SA), information systems security officers (ISSO), and users of the system. This document states individual's security responsibilities as users of the system.

1.2 Compliance

The DCS3000 Rules of Behavior are based on the principles described in the Computer Security Act of 1987 to protect sensitive information. More specific user responsibilities are set forth in the FBI Manual of Investigative Operations and Guidelines (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 DCS3000 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 DCS3000 or federal system security (and related) policy.

1.1.2 User Information and Contacts

Your supervisor or system administrator should furnish you with the following information when you are granted authorized user privileges on DCS3000. After that, it is your responsibility to stay up-to-date on the key personnel and phone numbers. You should know:

--

LIMITED OFFICIAL USE ONLY

-

- Your access privileges; your access privileges may be limited to a specific list of file areas, programs, and activities.

b6
b7C

You should know who the following individuals are and how to contact them:

Contact:	Description of Duties:	Telephone:
Project Manager <div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Project manager for DCS3000 activities.	[Redacted Telephone Numbers]
Information Systems Security Officer (ISSO) <div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Ensures that the information system is implemented with appropriate security features and meets the minimum security requirements.	
DCS3000 Senior System Technical Representative <div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Serves as senior technical advisor for all DCS3000 issues	
Switch-Based Intercept Program Manager <div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Serves as POC for all DCS3000 switch-based intercept issues	
User Representative <div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Serves as spokesman for all DCS3000 user issues.	
Supervisor (in the specific location)	Requests access for, or termination of service, to the Information system. Requests the establishment and deletion of directories.	

b6
b7C

Table 1: Contacts

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

1.1.3 The DCS3000 Environment

General Information

All DCS3000 users must read and abide by these rules of behavior.

All FBI ADPT systems are for official business only. System users have no expectation of privacy while utilizing these resources.

Sensitive and Classified Data Considerations

Classified national security information (i.e., Confidential, Secret or Top Secret information) will not be processed on any DCS3000.

All DCS3000 output that contains LOUO information will be so marked or labeled by the user who generated the material, and then stored or transmitted with appropriate protection. The designation "Limited Official Use Only" will be marked, stamped or permanently affixed to the top and bottom of the outside of the front and back covers (if any), on the title page and on all pages of documents or information requiring such control. All diskettes or other magnetic media containing sensitive information will be similarly labeled and stored in locked containers (e.g., desks, filing cabinets, etc.).

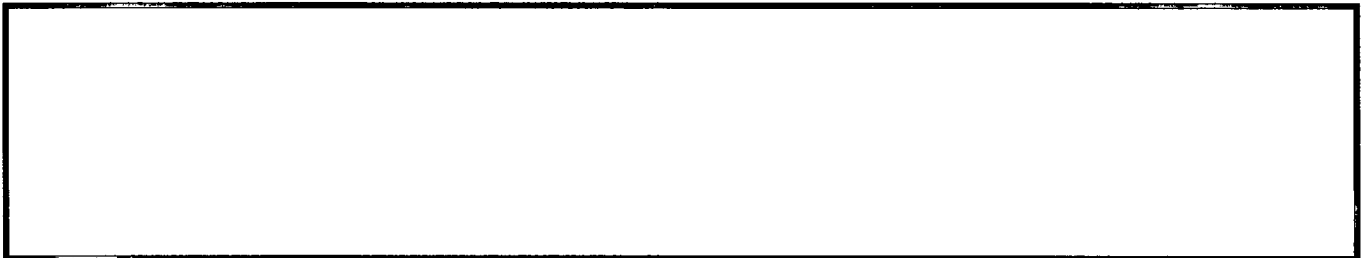
LOUO documents that are no longer needed should be shredded.

Magnetic media (e.g., diskettes and hard drives) that have been used for LOUO information may contain sensitive information even after the LOUO files are deleted. The information may be recoverable, even if a normal directory listing of the medium says it is empty. Before discarding magnetic media, users should do one of the following:

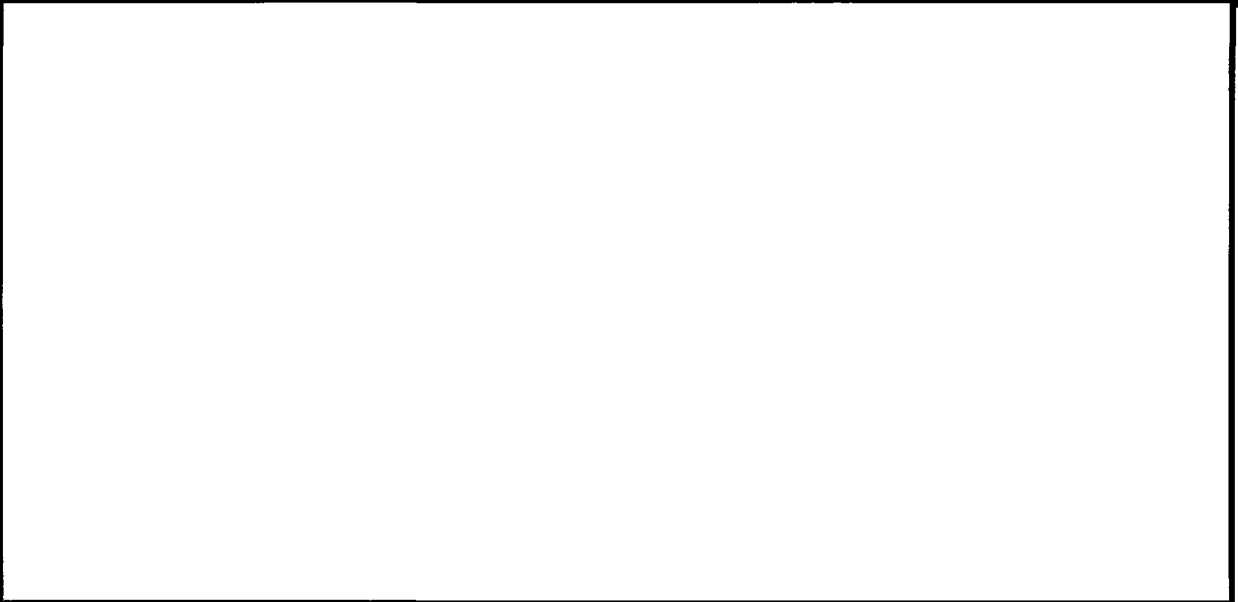
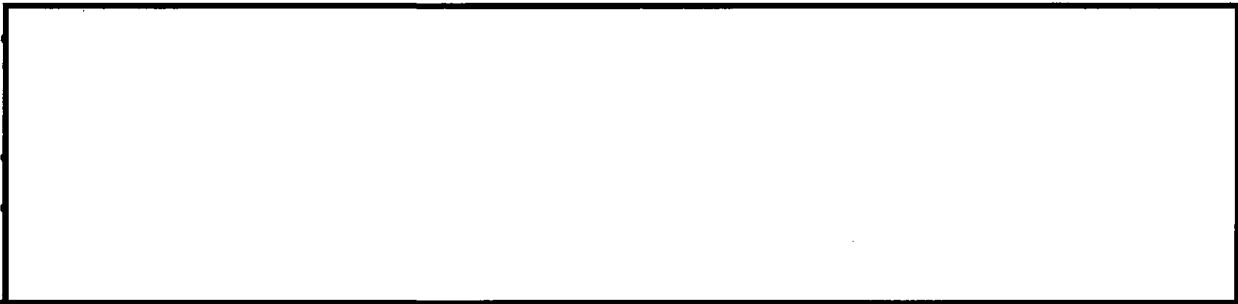
- 
- 
- 

If you need assistance in disposing of magnetic media, consult your system administrator or ISSO.

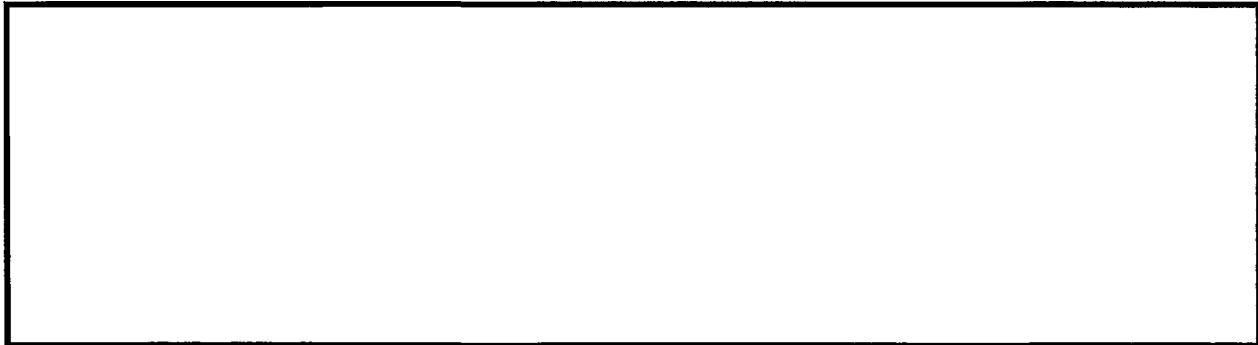
Passwords



LIMITED OFFICIAL USE ONLY



1.2 *Interacting With Administrators*



b2
b7E

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

- [Redacted]
- [Redacted]

[Redacted]

1.3 Configuration Management

[Redacted]

[Redacted]

b2
b7E

1.3.1 Things You May Change

[Redacted]

b2
b7E

1.3.2 Things You May Not Change

[Redacted]

LIMITED OFFICIAL USE ONLY

b2
b7E

1.4 Unauthorized Activities

[Redacted]

Unauthorized activities include:

[Redacted]

b2
b7E

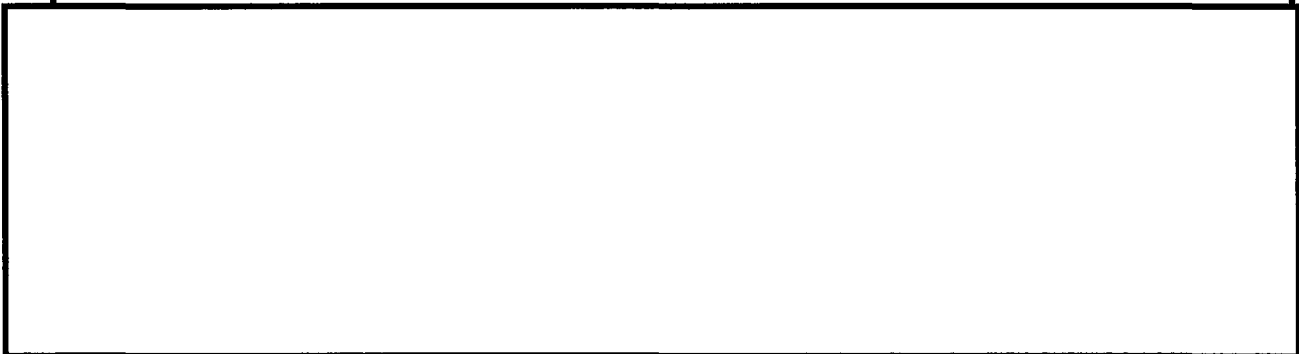
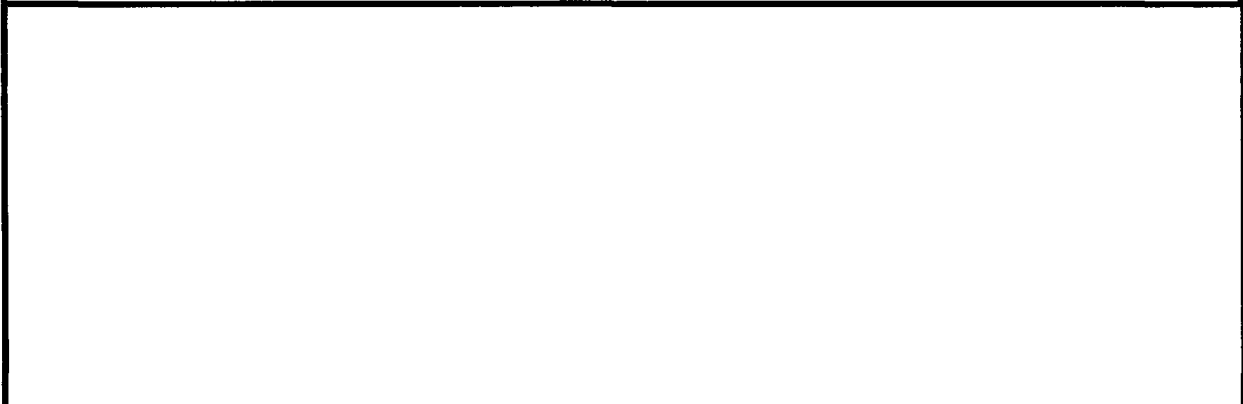
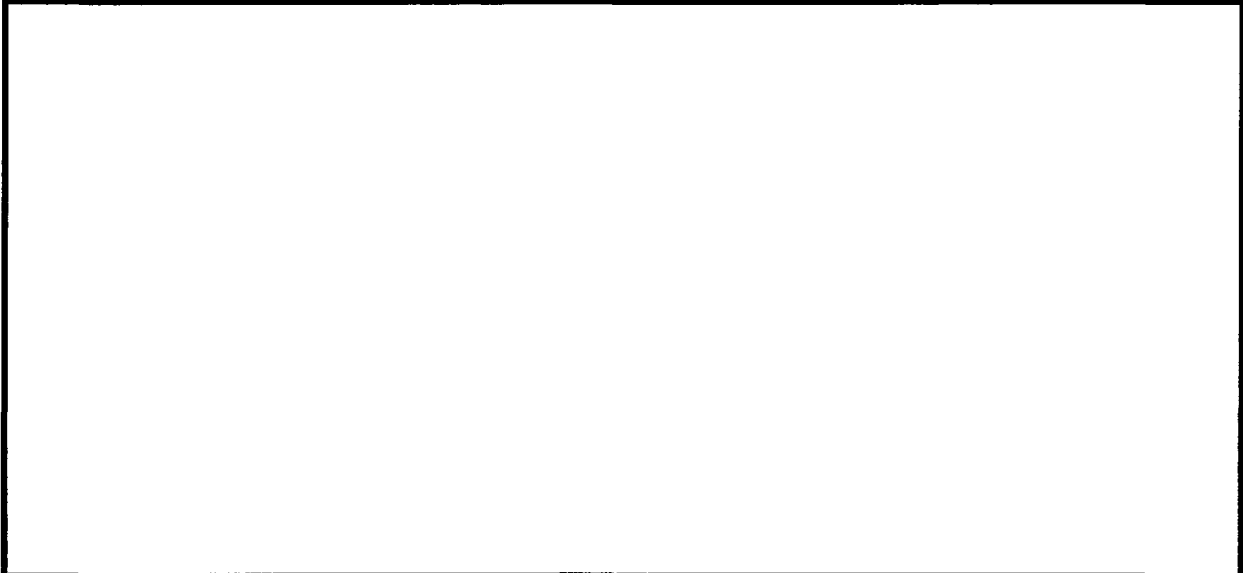
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

b2
b7E

LIMITED OFFICIAL USE ONLY

b2
b7E

1.5 Your Role in Protecting the System



b2
b7E

LIMITED OFFICIAL USE ONLY

2.0 USER SUPERVISORS

These Rules of Behavior apply to all supervisors of users of DCS3000.

b2
b7E

2.1 Account Creation Responsibilities

[Redacted content]

2.2 Account Termination Responsibilities

[Redacted content]

2.3 Account Parameters

[Redacted content]

2.4 Account Verification/Validation

[Redacted content]

2.5 Awareness Responsibilities

[Redacted content]

b2
b7E

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

[Redacted]

2.6 Official Use

[Redacted]

2.7 Incident Reporting

[Redacted]

b2
b7E

3.0 ADMINISTRATORS

[Redacted]

3.1 System Administrators

3.1.1 Responsibilities

[Redacted]

- [Redacted]

[Redacted]

- [Redacted]

- Becoming thoroughly familiar with and complying in all respects with the requirements of DCS3000 Security Policy and these Rules of Behavior.

b2
b7E

LIMITED OFFICIAL USE ONLY

b2
b7E

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]

[Redacted]

3.1.2 Separation of Duties

[Redacted]

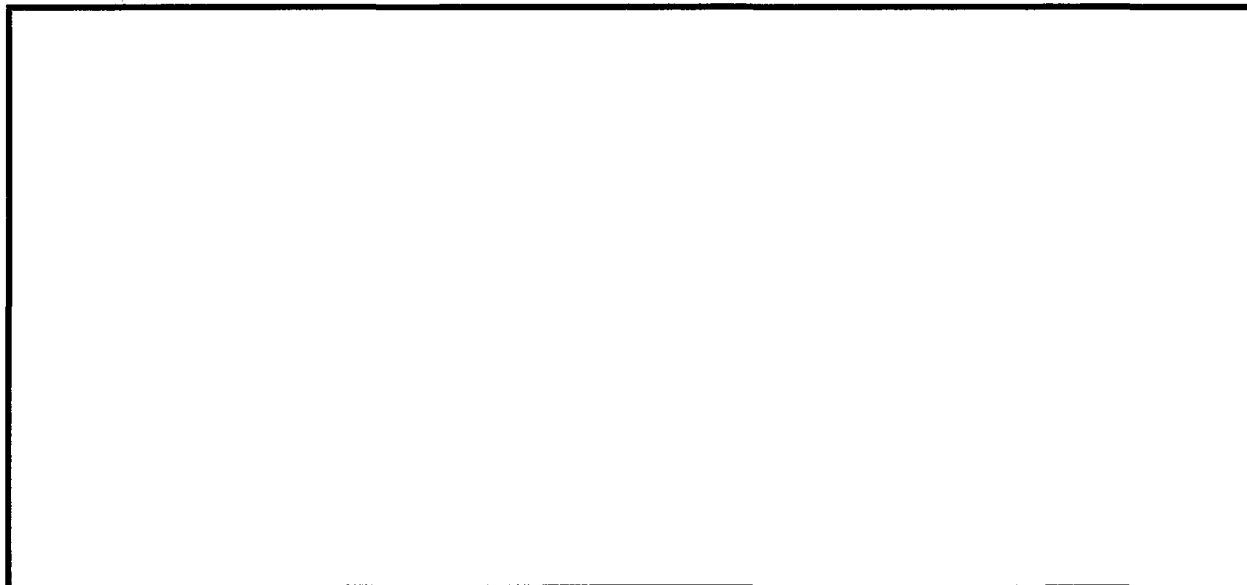
3.2 ISSO

The ISSO is responsible for:

b2
b7E

- [Redacted]
- [Redacted]
- [Redacted]

LIMITED OFFICIAL USE ONLY



4.0 INFORMATION SYSTEMS SECURITY MONITORING

This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. DCS3000 may be monitored routinely for indication of any unauthorized or malicious activity.

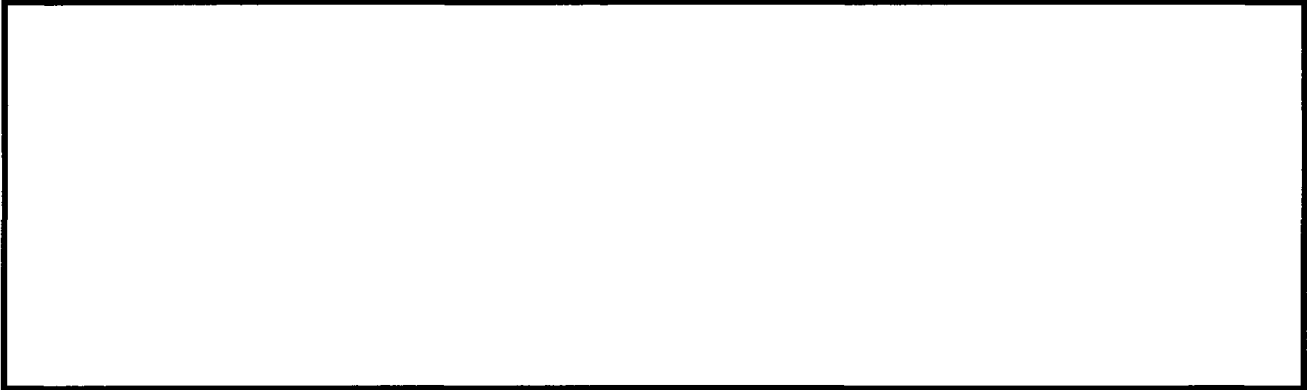
5.0 MONITORING NOTICES



b2
b7E

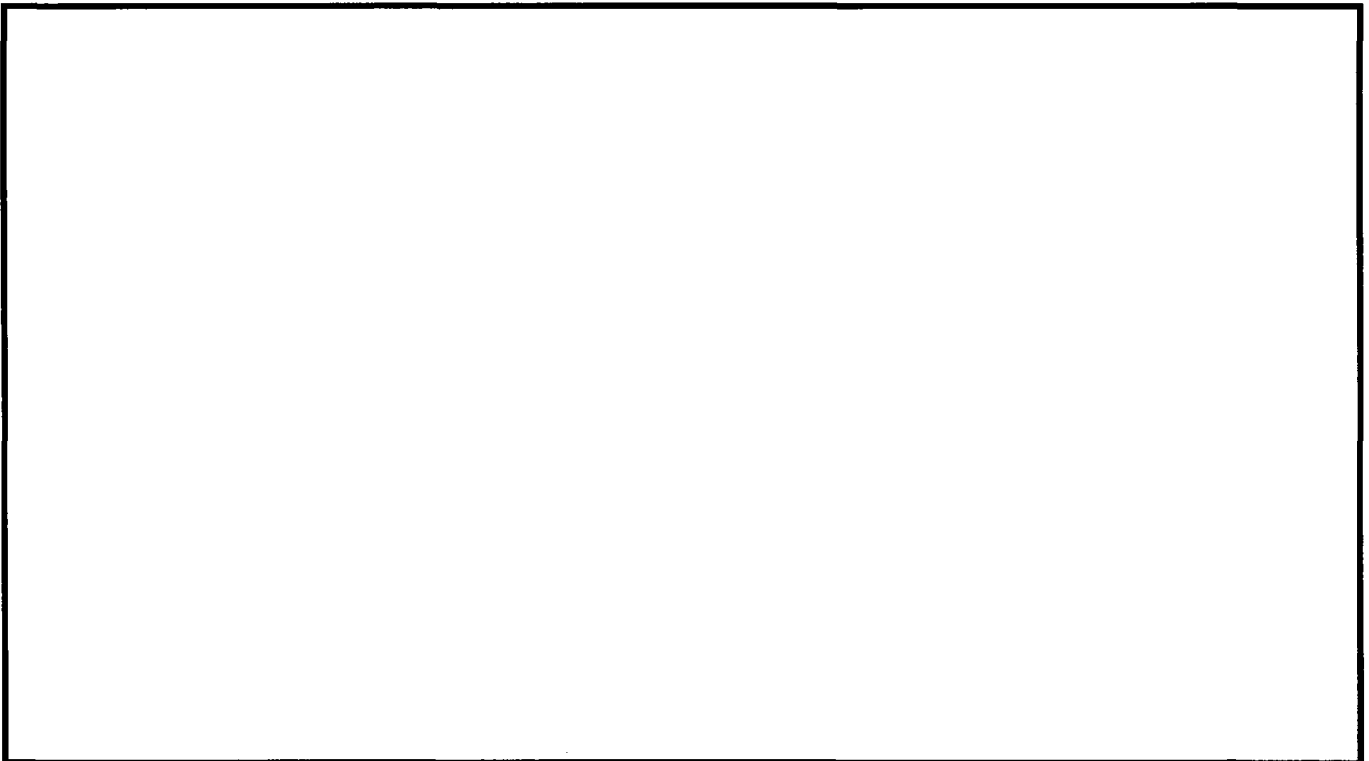
LIMITED OFFICIAL USE ONLY

5.1 Computer Log-on Banner



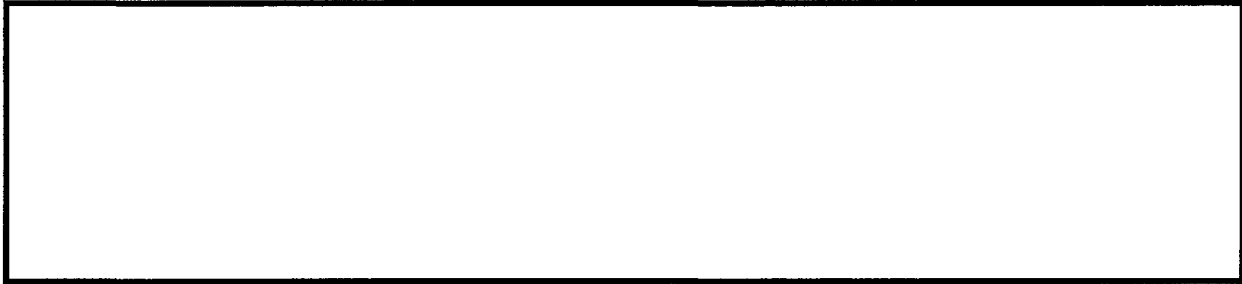
6.0 SYSTEM ADMINISTRATORS

6.1 Objective

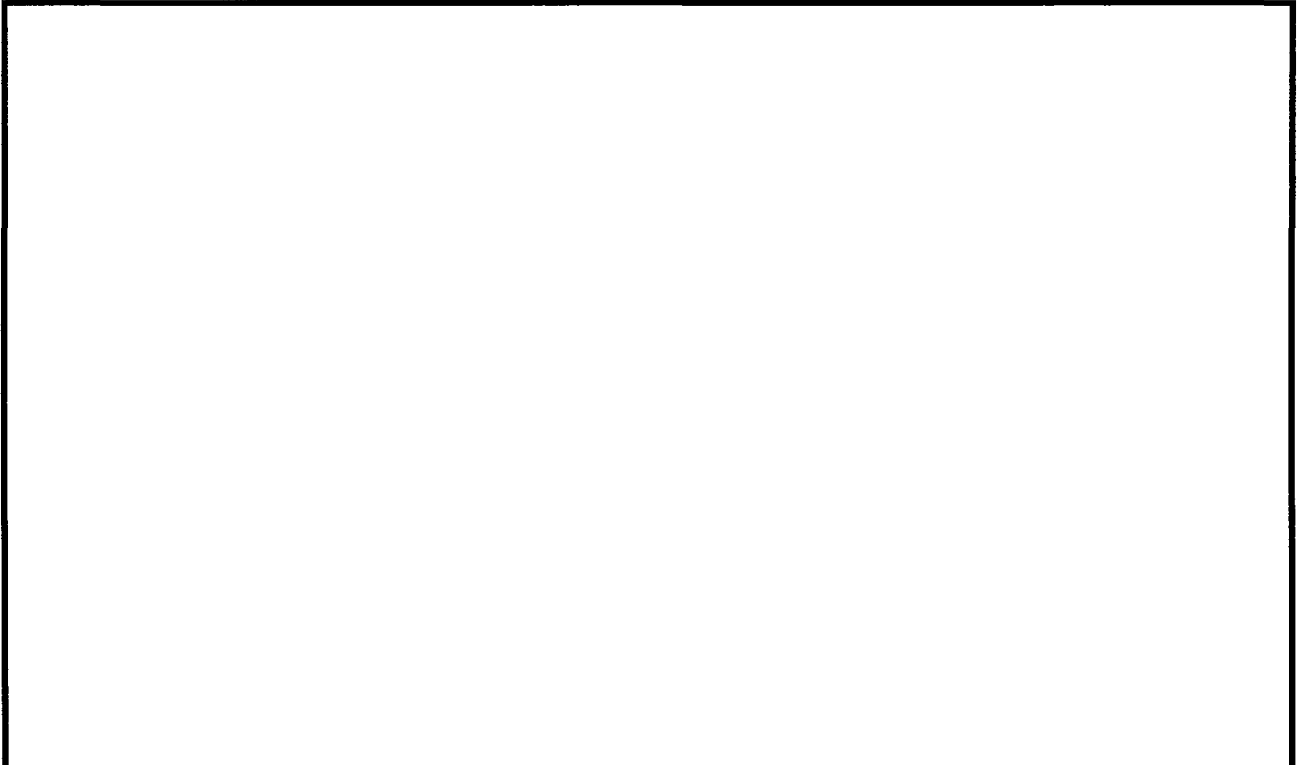


LIMITED OFFICIAL USE ONLY

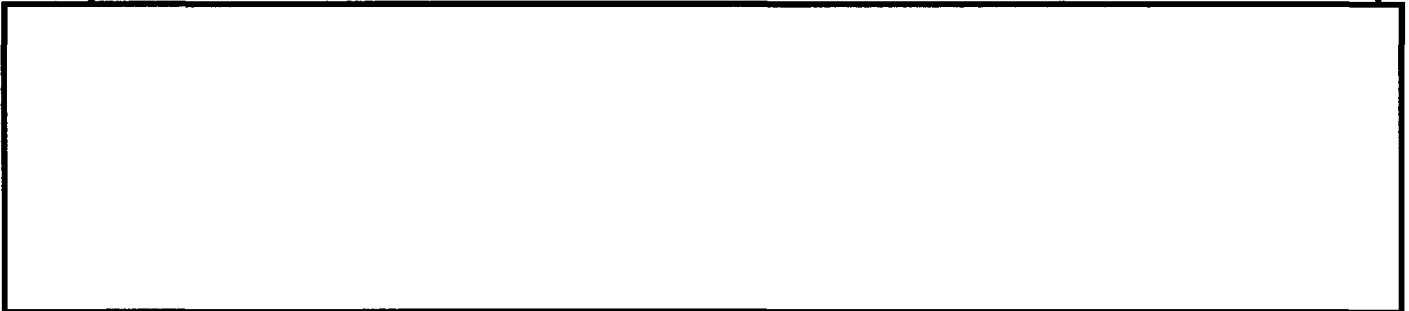
b2
b7E



6.2 *Restrictions on System Administrators in the Normal Performance of Their Duties*



b2
b7E



i

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

6.3 *Management Searches*

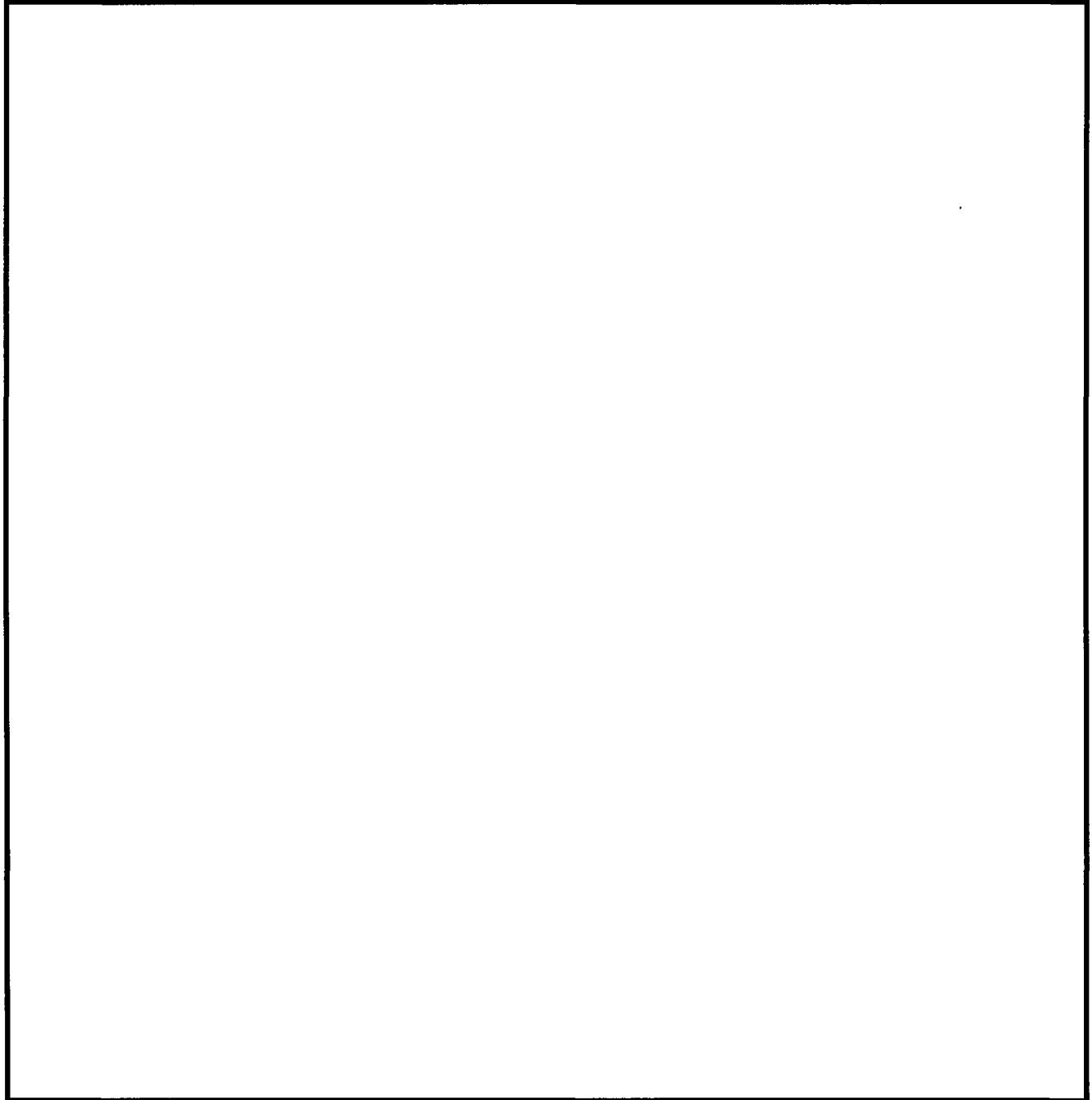
[Redacted content]

6.4 *Assistance to Law Enforcement and Counterintelligence*

[Redacted content]

LIMITED OFFICIAL USE ONLY

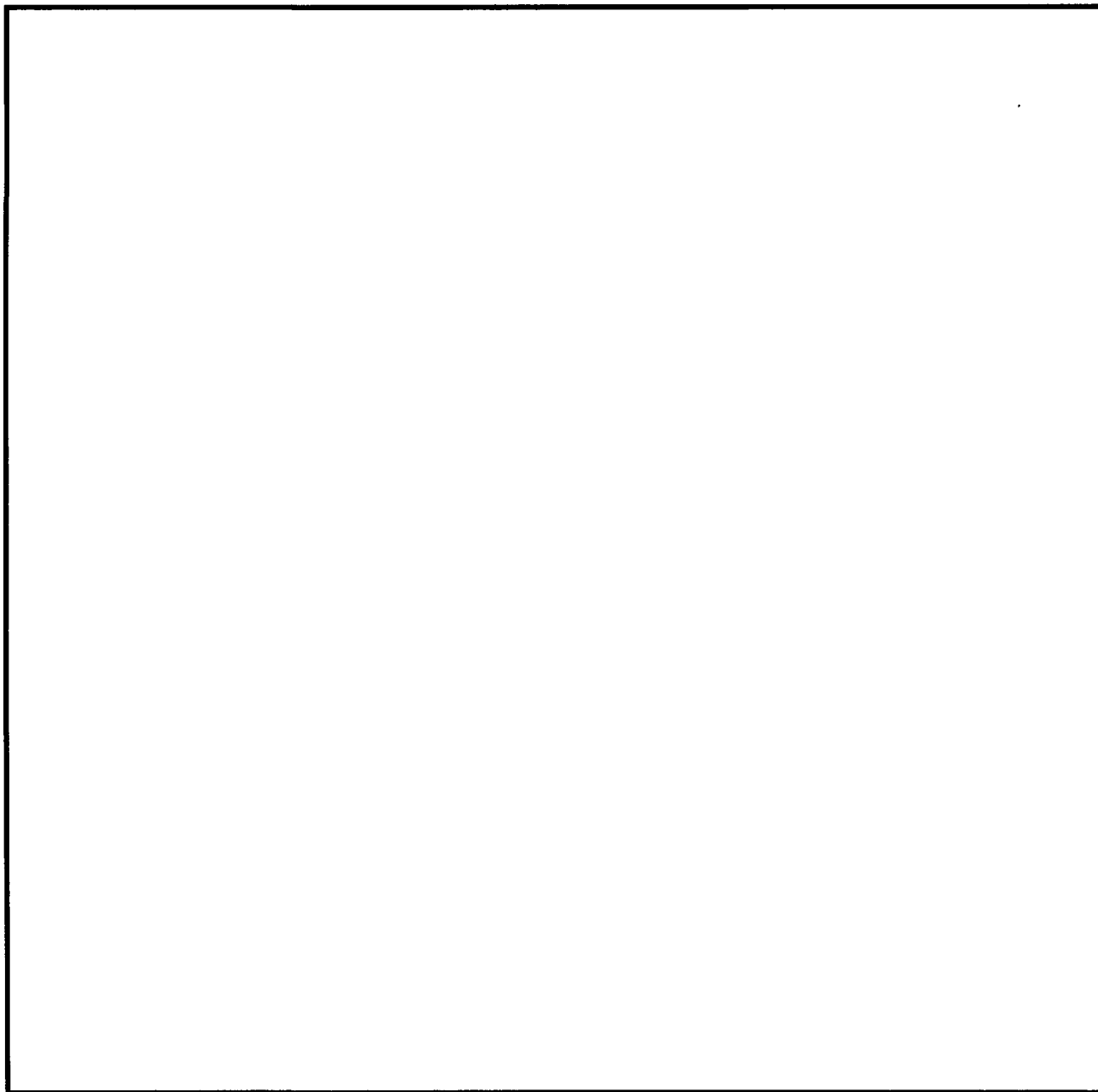
DCS3000/Privileged User Rules of Behavior Acknowledgement Form



i

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY



Privileged User Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

i

LIMITED OFFICIAL USE ONLY

Limited Official Use Only

Federal Bureau of Investigation
Field Office Integrated Security System
Appendix C - Rules of Behavior

i

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY



DCS3000
Appendix B
Security Concept of Operations
October 22, 2002
Version 1.0 – October 22, 2002

b6
b7C

Prepared For:

Chief, Legacy Systems Certification Unit (LSCU)
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Room 1302
Washington, DC 20530

Prepared By:
LSCU Green Team
FBIHQ

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65279 DMH/TAM/KSR/JB

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

TABLE OF CONTENTS

1. INTRODUCTION.....1
1.1. Purpose.....1
1.2. Background.....1
1.3. Project/Program Overview1
1.4. Assumptions1
2. REFERENCES1
3. CURRENT OPERATING ENVIRONMENT2
3.1. Current System.....2
3.2. Major System Components2
THE CLIENT.....2
THE SERVER.....2
THE MULTISERVER.....3
THE VANGUARD3
THE MULTI-VANGUARD.....3
3.3. User Organizations and Personnel.....3
4. SYSTEM OPERATIONAL OVERVIEW3
4.1. Networking Infrastructure3
4.2. Information Transfer and Collaboration.....6
4.3. Hardware.....6
4.4. Software.....6
4.5. Maintenance7
5. SECURITY.....7
5.1. System/Facility Access.....7
5.2. Physical Environment.....7
5.3. Data Storage Media.....7
5.4. Backup and Recovery8
6. POINTS OF CONTACT.....8

FIGURES

Figure 1. Typical DCS3000 Configuration – Pen Register4
Figure 2. Typical DCS3000 Configuration – Title III.....5

TABLES

Table 4-1. Sample Interconnection Configurations.....6

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

1. INTRODUCTION

The Data Collection System (DCS) 3000 application suite was developed to assist Law Enforcement Agencies (LEA) with collecting and processing data for Court-ordered electronic surveillance (ELSUR) operations. This system was developed, as an interim solution to Law Enforcement Agency collection needs until commercial collection platforms become available.

1.1. Purpose

The goal of this effort is to provide the Designated Accrediting Authority (DAA) with the information necessary to complete the security certification and accreditation (C&A) process. The C&A process validates that the required safeguards have been identified and implemented on the system. The culmination of this effort will be system accreditation (i.e. formal approval to operate) by the DAA.

1.2. Background

This security concept of operations (CONOPS) describes the planned operating conditions of the DCS3000 and the expected residual risk of operating the system. The system descriptions and security requirements provided herein are intended to assist the Designated Accrediting Authority (DAA) in determining the appropriate set of technical and non-technical safeguards for protecting the information in the DCS3000 system.

1.3. Project/Program Overview

[Redacted]

[Redacted]

The DCS3000 has been in operation since 1997 and is operational in [Redacted] FBI field offices across the United States.

b2
b7E

1.4. Assumptions

The security requirements described in this CONOPS are based on the following assumptions:

[Redacted]

2. REFERENCES

This document has been prepared in accordance with guidance provided by:

[Redacted]

3. CURRENT OPERATING ENVIRONMENT

3.1. Current System

[Redacted]

- **Pen Register** [Redacted]
- **Title III -** [Redacted]
- **Cooperative Warrant** [Redacted]

3.2. Major System Components

The DCS3000 suite consists of five component applications residing on one or more workstations. [Redacted]

[Redacted] The

DCS3000 consists of the following applications:

- Client
- Server
- MultiServer
- VANGuard
- MultiVANGuard

The Client

[Redacted]

The Server

[Redacted]

b2
b7E

The MultiServer

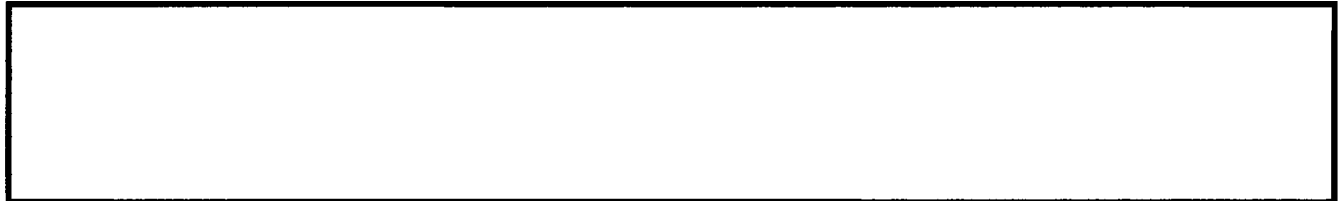


b2
b7E

The VANGuard



The Multi-VANGuard



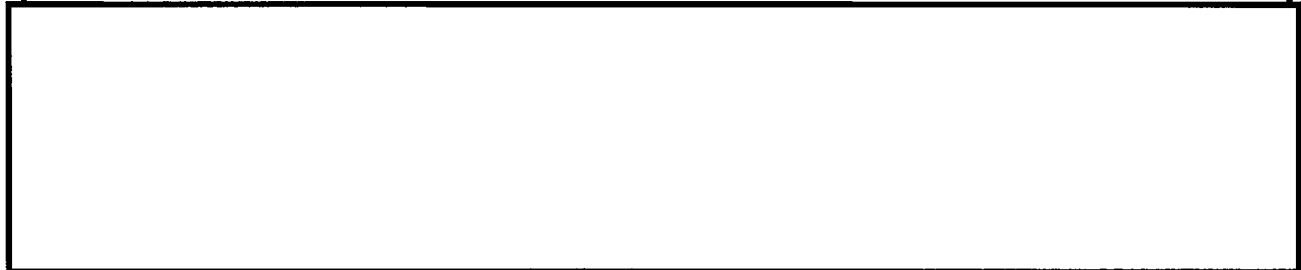
3.3. User Organizations and Personnel

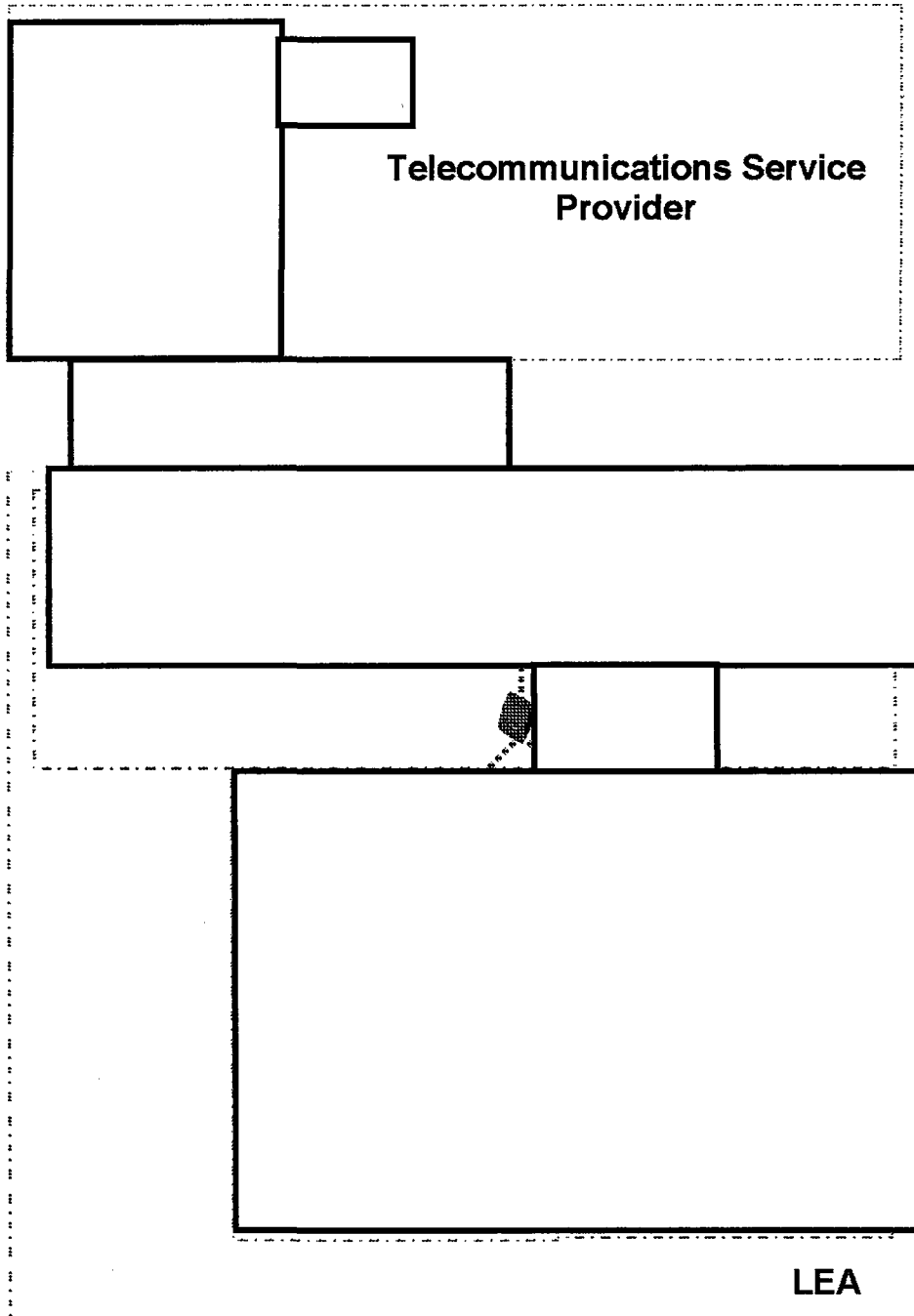


b2
b7E

4. SYSTEM OPERATIONAL OVERVIEW

4.1. Networking Infrastructure





b2
b7E

Figure 1. Typical DCS3000 Configuration – Pen Register

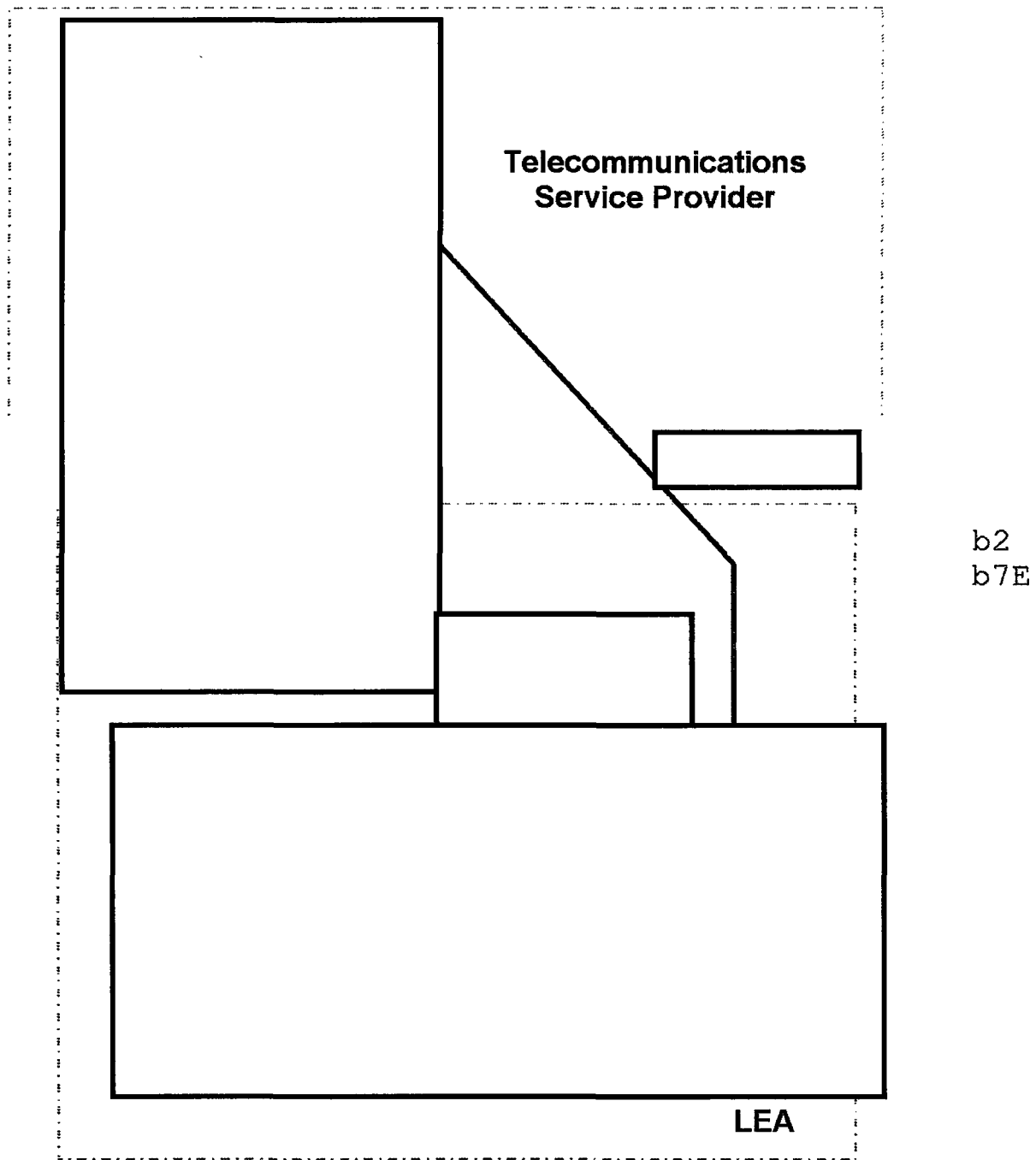


Figure 2. Typical DCS3000 Configuration – Title III

Table 4-1 represents sample data channel and content channel delivery mechanisms for telecommunications service providers.

Table 4-1. Sample Interconnection Configurations

Service Provider	Call Data Channel	Call Content Channel
[Redacted Table Content]		

b2
b7E

4.2. Information Transfer and Collaboration

[Redacted Content]

4.3. Hardware

The following subsections list and describe the major hardware required to operate the DCS3000 system.

4.3.1. Workstations

[Redacted Content]

[Redacted Content]

4.3.2. Data Communications Equipment

[Redacted Content]

4.4. Software

The following subsections list and describe the major software required to operate the DCS3000 system.

4.4.1. Operating System

[Redacted Content]

b2
b7E

4.4.2. DCS Applications

Please refer to section 3.1 above.

b2
b7E

4.4.3. Security Software

4.5. Maintenance

5. SECURITY

5.1. System/Facility Access

b2
b7E

5.2. Physical Environment

5.3. Data Storage Media

[Redacted]

5.4. Backup and Recovery

[Redacted]

[Redacted]

b2
b7E

6. POINTS OF CONTACT

[Redacted]

[Redacted]

Tele. No. 703 [Redacted]

[Redacted]

[Redacted]

Tele. No. 703 [Redacted]

b6
b7C

For Official Use Only

SECURITY EVALUATION REPORT

FOR THE

DCS3000

MARCH 27, 2003

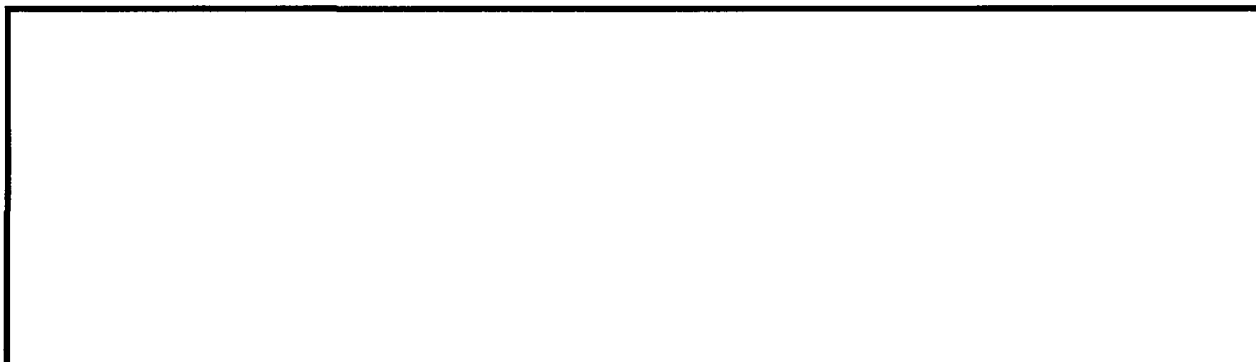
Prepared by:

b6
b7C


ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

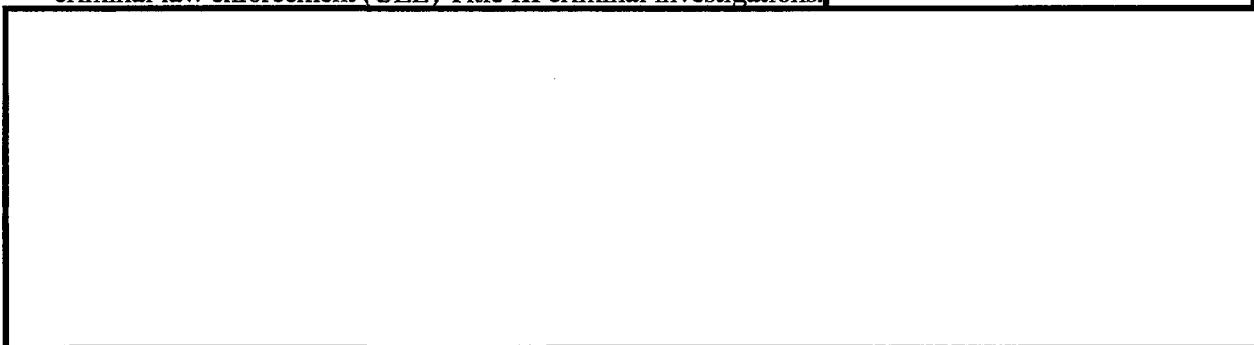
For Official Use Only

INTRODUCTION

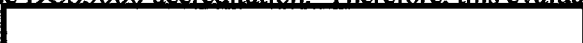


1. Background

The DCS3000 is an electronic surveillance (ELSUR) collection system that supports criminal law enforcement (CLE) Title III criminal investigations. 



b2
b7E

The system is used in several environments. FBI collection efforts and FBI/other federal, state or local agency joint collection efforts are controlled by FBI personnel. Although the FBI loans equipment and software to other law enforcement agencies for court ordered collections, the local agency is responsible for establishing and maintaining these collection efforts with the TSP. These standalone installations in local PDs, where the FBI provides no additional support or connectivity, are not a part of the DCS3000 accreditation. Therefore, this evaluation considers only equipment under FBI control 

DCS3000 data is collected in support of criminal cases and is protected as evidence 



b2
b7E

For Official Use Only

[Redacted]

Data that is passed through the DCS3000 must not be altered or lost, since it is collected for possible use as evidence in criminal cases. [Redacted]

[Redacted]

b2
b7E

During an investigation in which the DCS3000 is used, it is critical that the system is available at all times to record data. [Redacted]

[Redacted]

[Redacted]

[Redacted]

2. Evaluation of C&A Package

[Redacted]

b2
b7E

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b2
b7E

3. Statement of Residual Risk

[Redacted]

Vulnerability 1:

[Redacted]

Risk Impact:

[Redacted]

Current Mitigating Factors:

[Redacted]

[Redacted]

b2
b7E

Recommended Countermeasure:

[Redacted]

[Redacted]

For Official Use Only

Vulnerability 2:

[Redacted]

Risk Impact:

[Redacted]

[Redacted]

Current Mitigating Factors:

[Redacted]

[Redacted]

Recommended Countermeasure:

[Redacted]

[Redacted]

Vulnerability 3:

[Redacted]

Risk Impact:

[Redacted]

[Redacted]

Current Mitigating Factors:

[Redacted]

[Redacted]

Recommended Countermeasure:

[Redacted]

[Redacted]

4. Recommendation

[Redacted]

[Redacted]

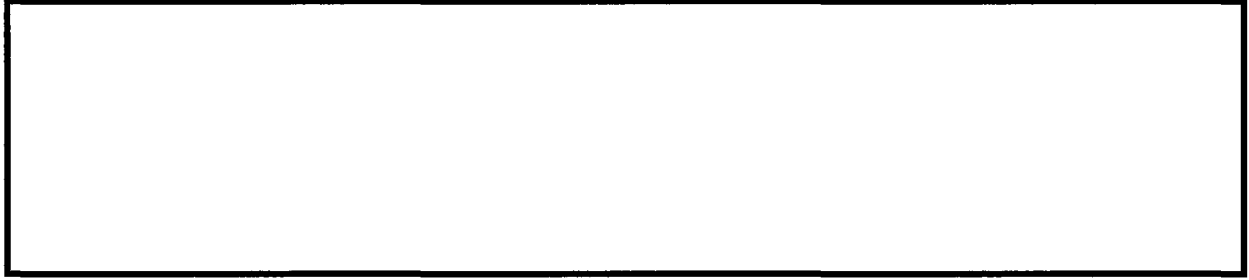
[Redacted]

b2
b7E

b2
b7E

b2
b7E

For Official Use Only



b2
b7E

For Official Use Only

FOR OFFICIAL USE ONLY

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

FOR OFFICIAL USE ONLY

Table of Contents

INTRODUCTION.....6

1. INFORMATION SYSTEM GENERAL INFORMATION7

 1.1 *Security Administration*.....7

 1.1.1 System Information.....7

 1.1.2 Key System Points of Contact7

 1.1.3 Security Organization9

 1.2 *Mission*.....9

 1.2.1 Purpose and Scope.....9

 1.2.2 Supported Projects9

 1.2.3 Information System Usage.....9

 1.3 *Inter-Departmental/Agency Use and Agreements*.....10

 1.3.1 Joint Use Information10

 1.3.2 Memorandum of Agreement (MOA)/Understanding (MOU).....10

 1.3.3 Interconnection Security Agreement (ISA)10

2. SECURE FACILITY DESCRIPTION.....11

 2.1 *Facility Layout*.....11

 2.2 *Physical and Environmental Protection*.....12

 2.2.1 Physical Protection12

 2.2.2 Environmental Protection12

 2.3 *System Layout*.....13

 2.4 *Emanation Protection*.....13

 2.4.1 Red/Black Separation.....13

 2.4.2 TEMPEST13

3. SYSTEM DESCRIPTION.....14

 3.1 *Summary*.....14

 3.2 *Mode of Operations*.....16

 3.3 *Level of Concern*.....16

 3.3.1 Confidentiality16

 3.3.2 Integrity16

 3.3.3 Availability16

 3.4 *Tier Level Designation*.....16

 3.5 *System Diagram*.....17

 3.6 *Interconnection Interface Description*.....17

 3.6.1 Direct Network Connections17

 3.6.2 Indirect Connections21

 3.7 *Data Processed*.....21

 3.7.1 Classification and Compartments.....21

 3.7.2 Dissemination Controls22

 3.7.3 Type of Data Processed.....22

 3.8 *Data Flow Diagram*.....22

4. SYSTEM HARDWARE24

 4.1 *Hardware List*.....24

FOR OFFICIAL USE ONLY

4.2 *Hardware Labeling*.....24
 4.2.1 *Labeling of System Hardware*24
 4.2.2 *Exceptions*.....24
4.3 *Sanitization and Destruction*.....24
4.4 *Custom-Built Hardware*.....25
5.0 SYSTEM SOFTWARE.....26
 5.1 *Software List*.....26
 5.2 *Software with Restricted Access or Limited Use Requirements*.....26
 5.3 *Foreign Software*.....27
 5.4 *Freeware/Shareware/Open-Source Software*27
 5.5 *Marking and Labeling*.....27
6. DATA STORAGE MEDIA.....28
 6.1 *Media Type*.....28
 6.2 *Media Handling*28
 6.2.1 *Media Introduction and Removal*28
 6.2.2 *Sanitization and Destruction*.....29
 6.3 *Storage Media Marking and Labeling*.....29
7. SECURITY CONTROL REQUIREMENTS.....30
 7.1 *Management*.....30
 7.1.1 *Risk Assessment*.....30
 7.1.2 *Compliance and Monitoring Program*.....30
 7.2 *Operational*31
 7.2.1 *Personnel Security*.....31
 7.2.2 *Contingency Planning*.....33
 7.2.3 *Configuration Management Program*.....35
 7.2.4 *Maintenance*37
 7.2.5 *System & Information Integrity*.....40
 7.2.6 *User's Guides*41
 7.2.7 *Incident Response*.....42
 7.3 *Technical*.....43
 7.3.1 *Access Control*43
 7.3.2 *Identification & Authentication*.....46
 7.3.3 *Accountability (Including Audit Trails)*49
 7.3.4 *System & Communications Protection*.....53
8. SECURITY AWARENESS PROGRAM.....56
 8.1 *Program Description*.....56
 8.2 *Rules of Behavior*.....57
9. EXCEPTIONS.....58
10. GLOSSARY OF TERMS.....59

List of Figures

Figure 1: DCS 3000 Data Flow23
Figure 2: Organization Structure for DCS 3000 Program Management.....61
Figure 3: Typical DCS 3000 Configuration.....62

List of Tables

Table 1: Equipment List.....24
Table 2: DCS 3000 Software26
Table 3: DCS 3000 Application Version Numbers.....26

Attachments

- Attachment A – Type Organizational Structure
- Attachment B – Type Detailed System Diagrams

FOR OFFICIAL USE ONLY

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. [REDACTED]

[REDACTED]

b2
b7E

FOR OFFICIAL USE ONLY

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		
Revision/Version		
TSABI Number (if applicable)	Not Applicable (N/A)	
Web Location for documentation (if applicable)		b2
Status (New System or Modification to an Existing System)?		b7E
Project ID (if applicable)	N/A	
Deployment Installation Date		
Security Test & Evaluation Date		
Required Operational Date		

1.1.2 Key System Points of Contact

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

FOR OFFICIAL USE ONLY

	Email Address	
Certifier	Name	
	Organization	
	Address	
	Phone: Commercial	
	Phone: Secure	
	Pager	
	Email Address	
	ISSM	Name
Organization		
Address		
Phone: Commercial		
Phone: Secure		N/A
Pager		N/A
Email Address		[Redacted]
ISSO		Name
	Organization	TICTU
	Address	ERF Building #27958-A Quantico, VA 22135
	Phone: Commercial	[Redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[Redacted]
	ISSO Alternate	Name
Organization		TICTU
Address		[Redacted]
Phone: Commercial		[Redacted]
Phone: Secure		N/A
Pager		N/A
Email Address		[Redacted]
System Administrator		Name
	Organization	TICTU
	Address	[Redacted]
	Phone: Commercial	[Redacted]
	Phone: Secure	N/A
	Pager	N/A
	Email Address	[Redacted]

b6
b7C

FOR OFFICIAL USE ONLY

1.1.3 Security Organization

[Redacted]

1.2 Mission

1.2.1 Purpose and Scope

[Redacted]

[Redacted]

[Redacted]

b2
b7E

1.2.2 Supported Projects

PROJECT NAME	CLASSIFICATION & CONTROLS	PROJECT POC
[Redacted]	[Redacted]	[Redacted]

b6
b7C

The DCS 3000 is an ELSUR collection system.

1.2.3 Information System Usage

[Redacted] Briefing Boards	[Redacted] Network Management	[Redacted] Data Collection
[Redacted] Communications	[Redacted] Presentations	[Redacted] Data Processing
[Redacted] Collaborative Computing	[Redacted] Software Development	[Redacted]
[Redacted] Database	[Redacted] Prototyping	[Redacted]
[Redacted] Data Release	[Redacted] Signals Processing	[Redacted]

b2
b7E

FOR OFFICIAL USE ONLY

b2
b7E

E-Mail	Spreadsheets	<input type="checkbox"/>
Image Processing	Web/Web Design	<input type="checkbox"/>
Mapping	Word Processing	<input type="checkbox"/>

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

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Diagrams and supporting documents for each FBI office which houses a DCS 3000 system

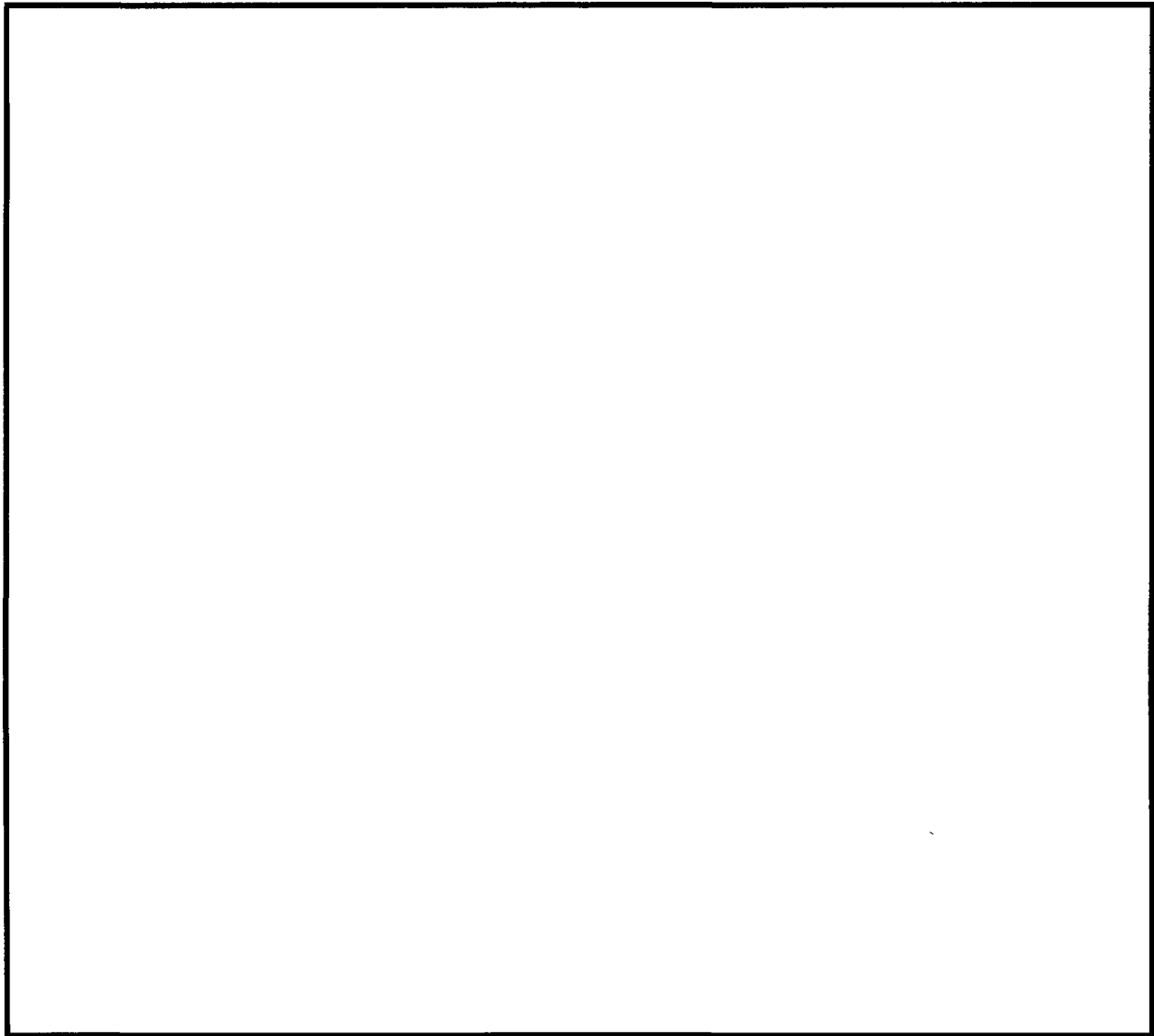
[Redacted]

b2
b7E

b2
b7E

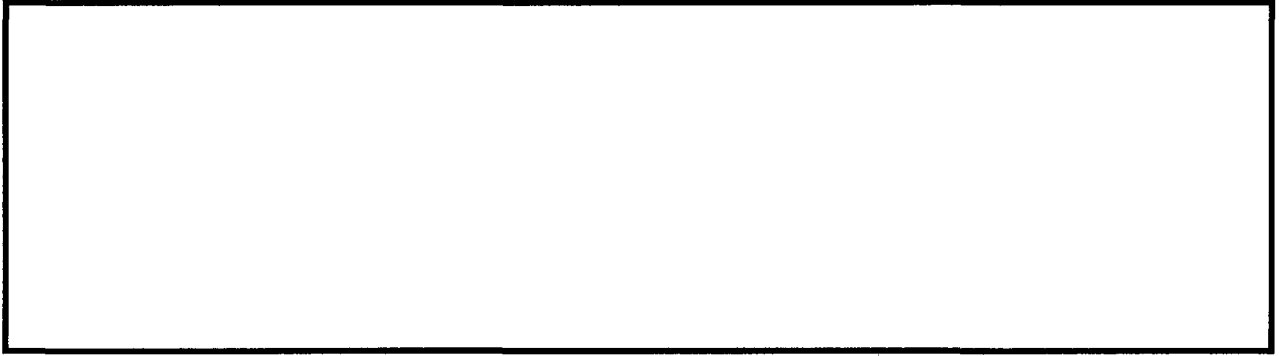
2.2 Physical and Environmental Protection

2.2.1 Physical Protection



2.2.2 Environmental Protection





b2
b7E

2.3 System Layout



2.4 Emanation Protection

2.4.1 Red/Black Separation



2.4.2 TEMPEST

The DCS 3000 system is not subject to TEMPEST requirements.

b2
b7E

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]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

b2
b7E

[Redacted] used to connect the DCS 3000 to the TSPs' switches. [Redacted]
[Redacted] utilized to connect the various DCS 3000 installations to each other.
[Redacted] typical configuration of the DCS 3000 system.

b2
b7E

Operating System:

The DCS 3000 Client [Redacted]
[Redacted] the Server, Multiserver, VANGuard, and MultiVANGuard [Redacted]

[Redacted]

Perimeter:

b2
b7E

[Redacted]

[Redacted]

User Population:

b2
b7E

[Redacted]

[Redacted] DCS 3000 User Guide. In addition, the following documents have been generated [Redacted] 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:

b2
b7E

[Redacted]

Data Flow and Controls

[Redacted]

3.2 Mode of Operations

b2
b7E

<input type="checkbox"/> Dedicated System High	<input type="checkbox"/> Compartmented Multi-Level
---	---

3.3 Level of Concern

3.3.1 Confidentiality

b2
b7E

<input type="checkbox"/> Basic	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--------------------------------	---------------------------------	-------------------------------

3.3.2 Integrity

<input type="checkbox"/> Basic	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--------------------------------	---------------------------------	-------------------------------

3.3.3 Availability

<input type="checkbox"/> Basic	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--------------------------------	---------------------------------	-------------------------------

3.4 Tier Level Designation

<input type="checkbox"/> Tier 1	<input type="checkbox"/> Tier 2	<input type="checkbox"/> Tier 3	<input type="checkbox"/> Tier 4
---------------------------------	---------------------------------	---------------------------------	---------------------------------

b2
b7E

3.5 System Diagram

b2
b7E

3.6 Interconnection Interface Description

3.6.1 Direct Network Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY

b2
b7E

3.6.1.1 Connectivity Management Procedures

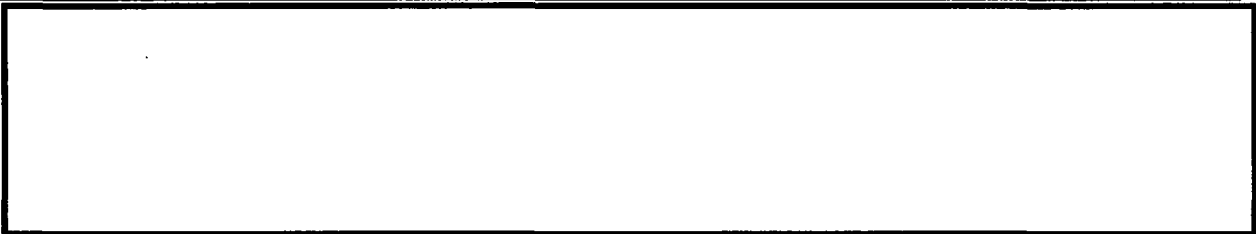
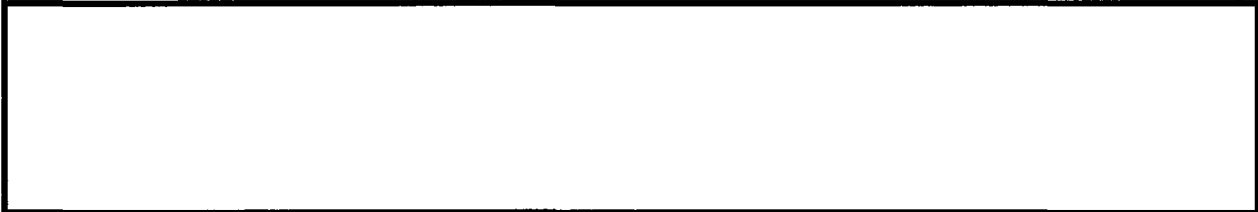
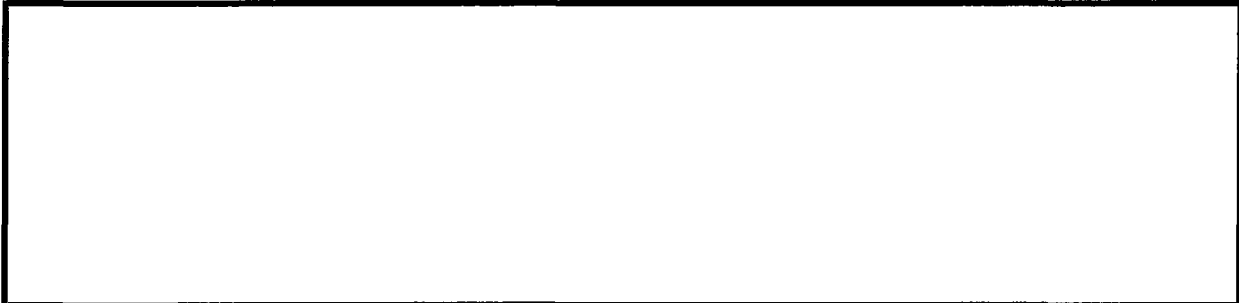
Overall:



b2
b7E

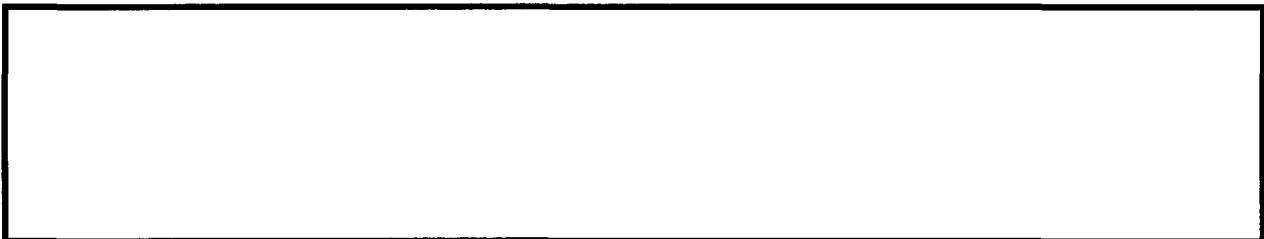
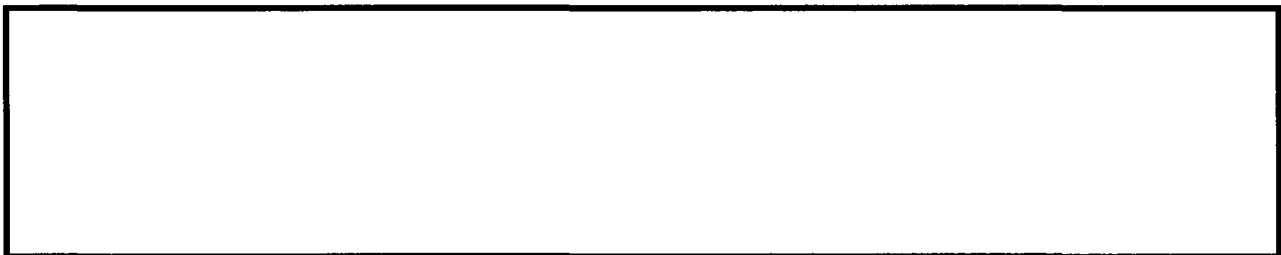
See Section 7.2.3 for further information on the DCS 3000 Configuration Management Plan.

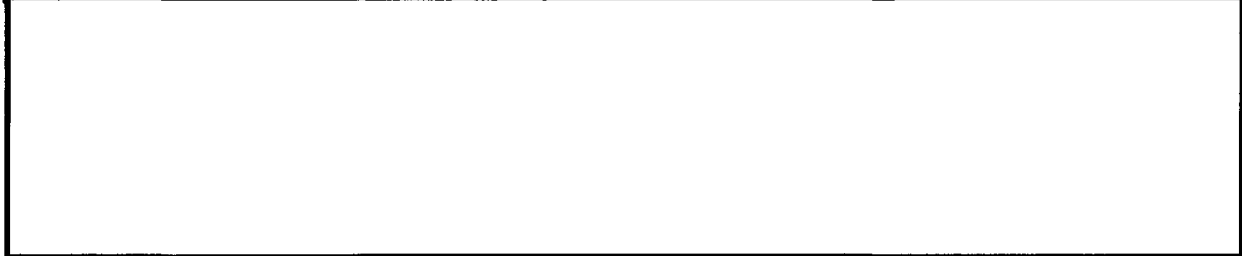
External Connectivity:



b2
b7E

3.6.1.2 Interconnection

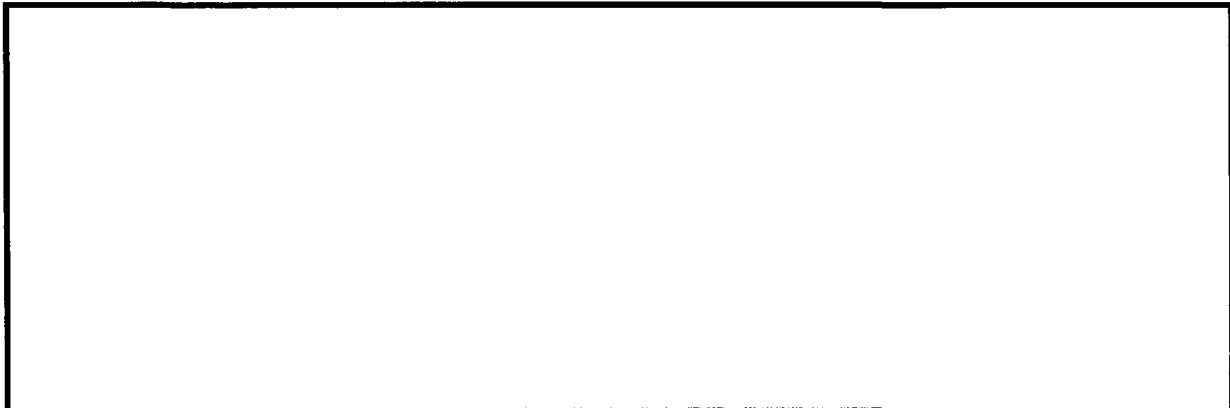




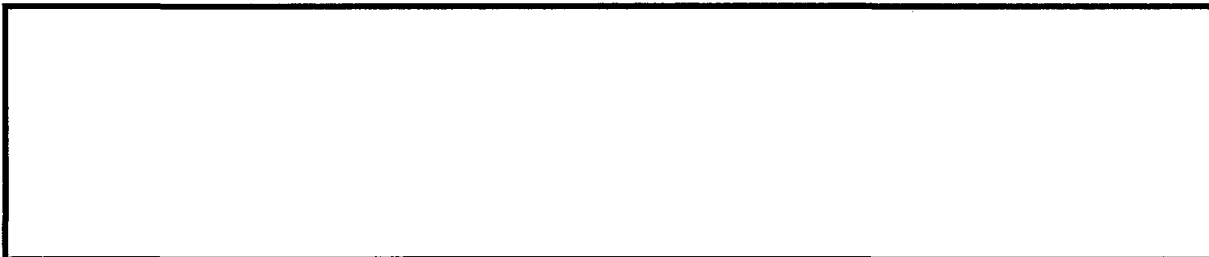
b2
b7E

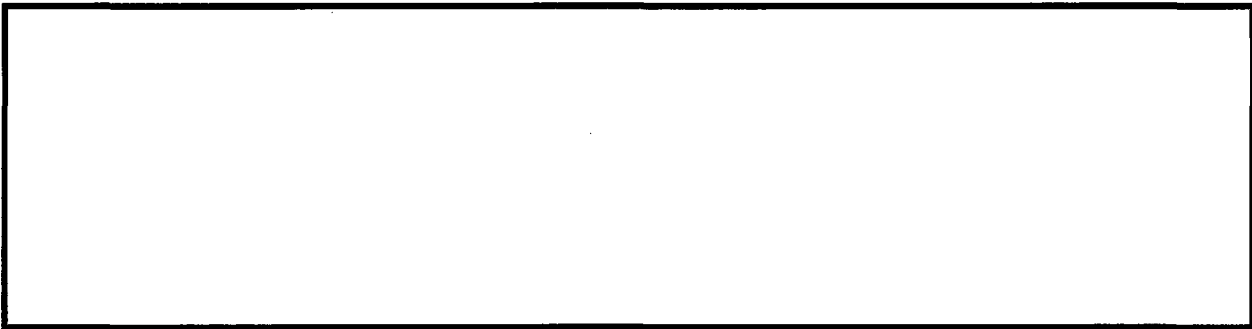


3.6.1.3 Connectivity Procedures

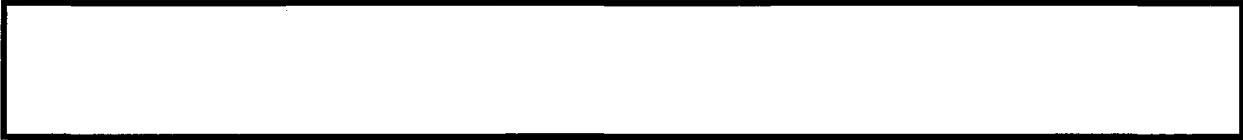


b2
b7E

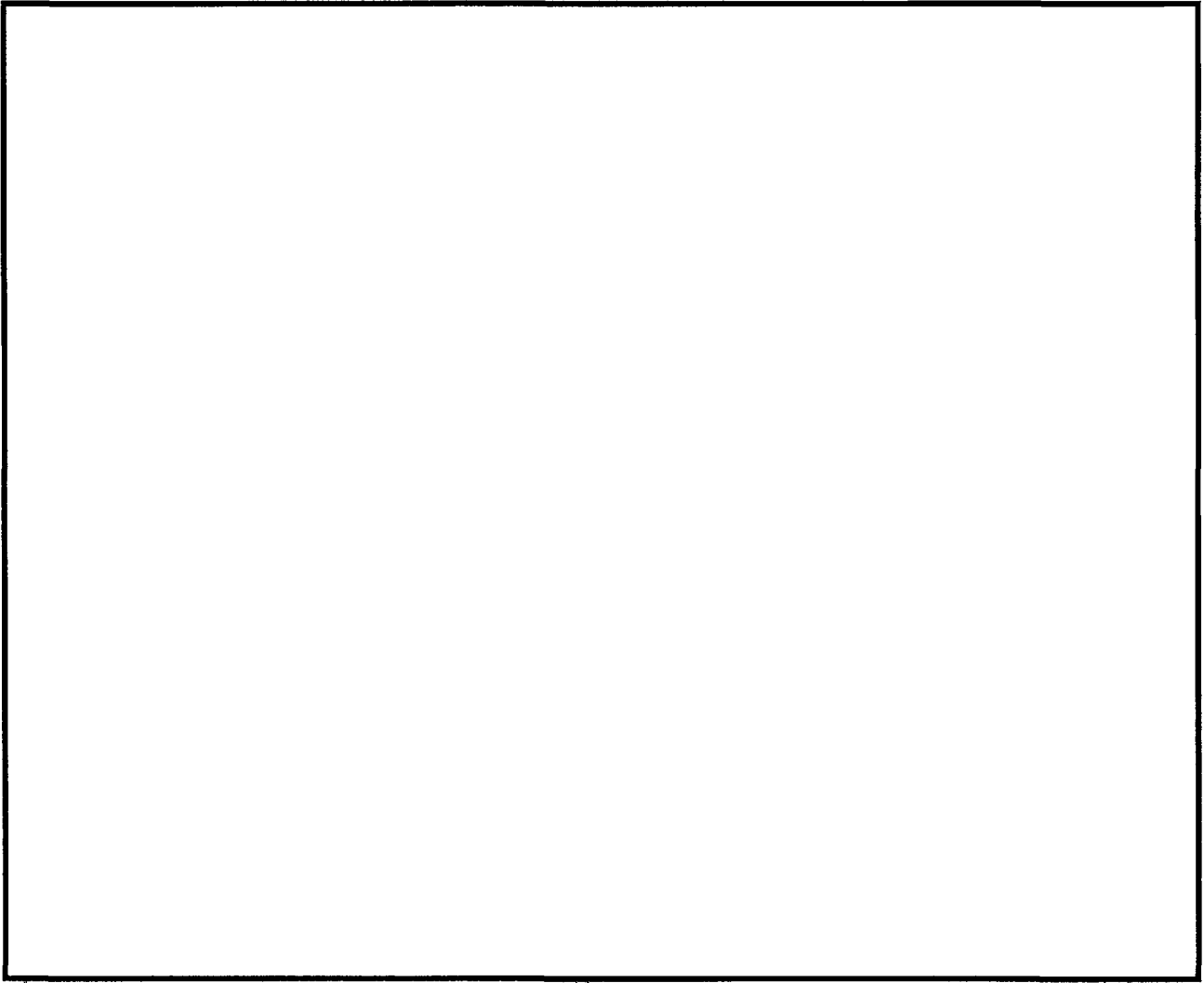




b2
b7E



3.6.1.4 Networking



b2
b7E

3.6.2 Indirect Connections

3.6.2.1 Indirect Import

3.6.2.2 Indirect Export

b2
b7E

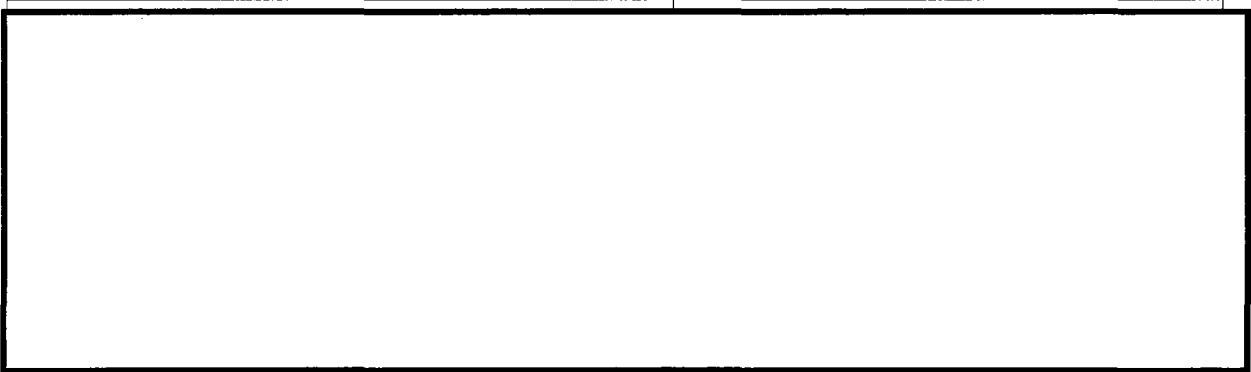
SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
-------------	-------------------------------	---------------	-----------------

3.7 Data Processed

3.7.1 Classification and Compartments

b2
b7E

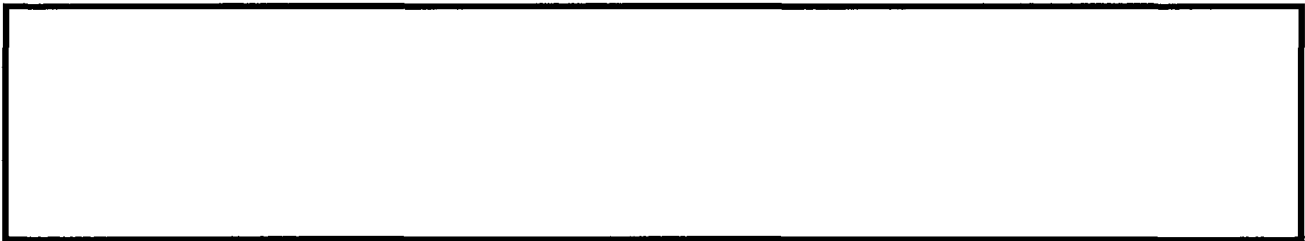
3.7.2 Dissemination Controls



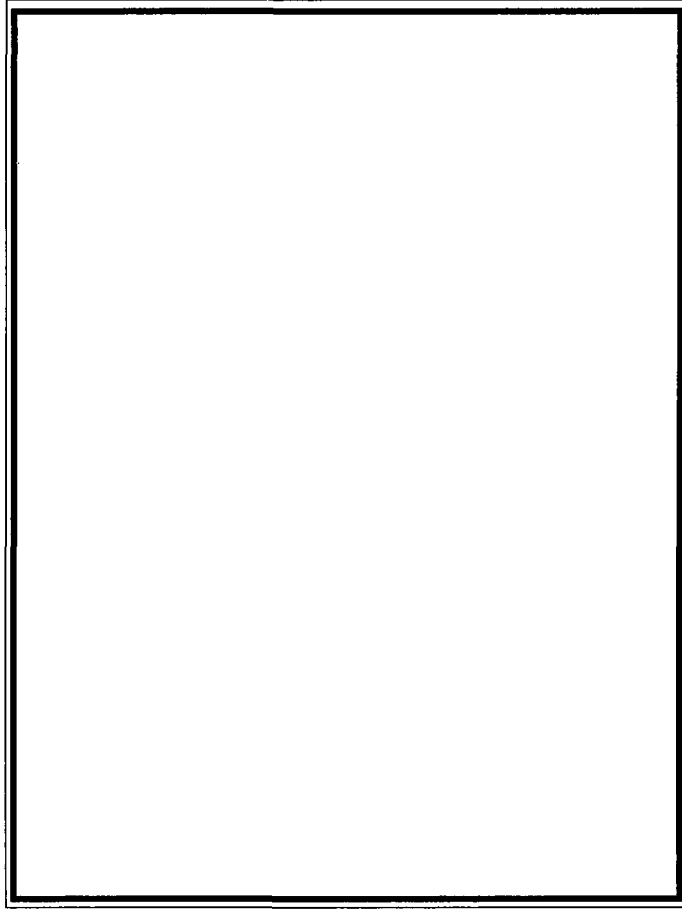
3.7.3 Type of Data Processed

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



FOR OFFICIAL USE ONLY



b2
b7E

Figure 1: DCS 3000 Data Flow

FOR OFFICIAL USE ONLY

4. SYSTEM HARDWARE

4.1 Hardware List

b2
b7E

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
[Redacted Table Content]					

Table 1: Equipment List

[Redacted Table Content]

4.2 Hardware Labeling

4.2.1 Labeling of System Hardware

[Redacted Content]

4.2.2 Exceptions

[Redacted Content]

b2
b7E

4.3 Sanitization and Destruction

[Redacted Content]



4.4 Custom-Built Hardware



b2
b7E

5.0 SYSTEM SOFTWARE

5.1 Software List

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

Name	Version	Manufacturer	Intended Use or Function
[Redacted]			

Table 2: DCS 3000 Software

b2
b7E

DCS Application Component	Version
[Redacted]	

Table 3: DCS 3000 Application Version Numbers

[Redacted]

5.2 Software with Restricted Access or Limited Use Requirements

[Redacted]

5.3 Foreign Software

[Redacted]

5.4 Freeware/Shareware/Open-Source Software

b2
b7E

[Redacted]

5.5 Marking and Labeling

[Redacted]

6. DATA STORAGE MEDIA

6.1 Media Type

--

TYPE OF MEDIA	SECURITY CONTROLS
---------------	-------------------

--	--

Removable Media

TYPE OF MEDIA	SECURITY CONTROLS
---------------	-------------------

--	--

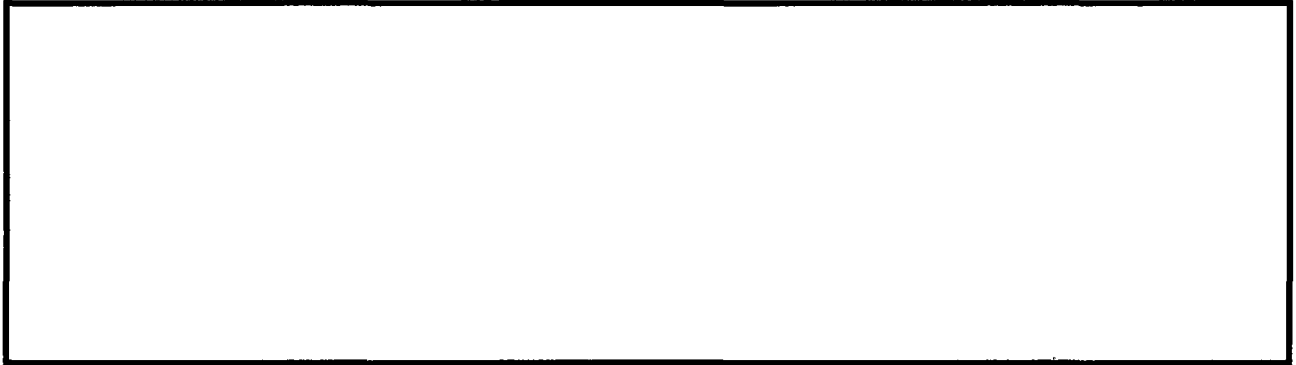
Non-Removable Media

6.2 Media Handling

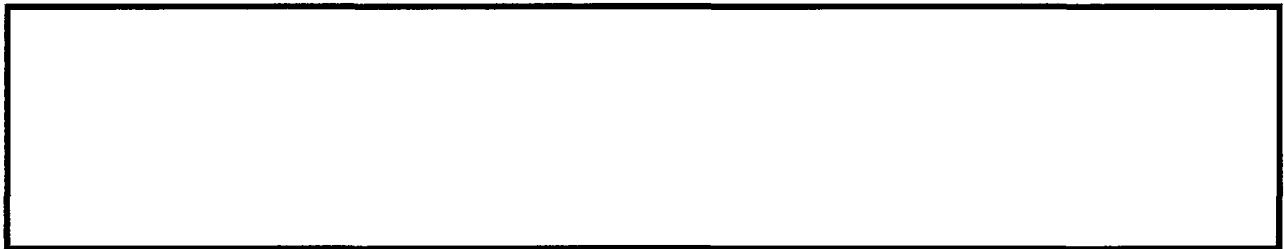
6.2.1 Media Introduction and Removal

--

6.2.2 Sanitization and Destruction



6.3 Storage Media Marking and Labeling



b2
b7E

7. SECURITY CONTROL REQUIREMENTS

b2
b7E

7.1 Management

7.1.1 Risk Assessment

7.1.2 Compliance and Monitoring Program

b2
b7E

[Redacted]

[Redacted]

b2
b7E

[Redacted]

[Redacted]

7.2

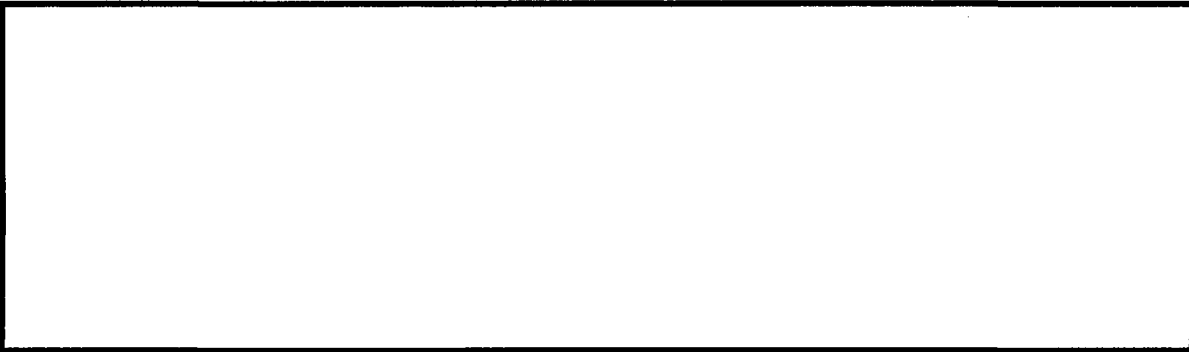
[Redacted]

7.2.1 Personnel Security

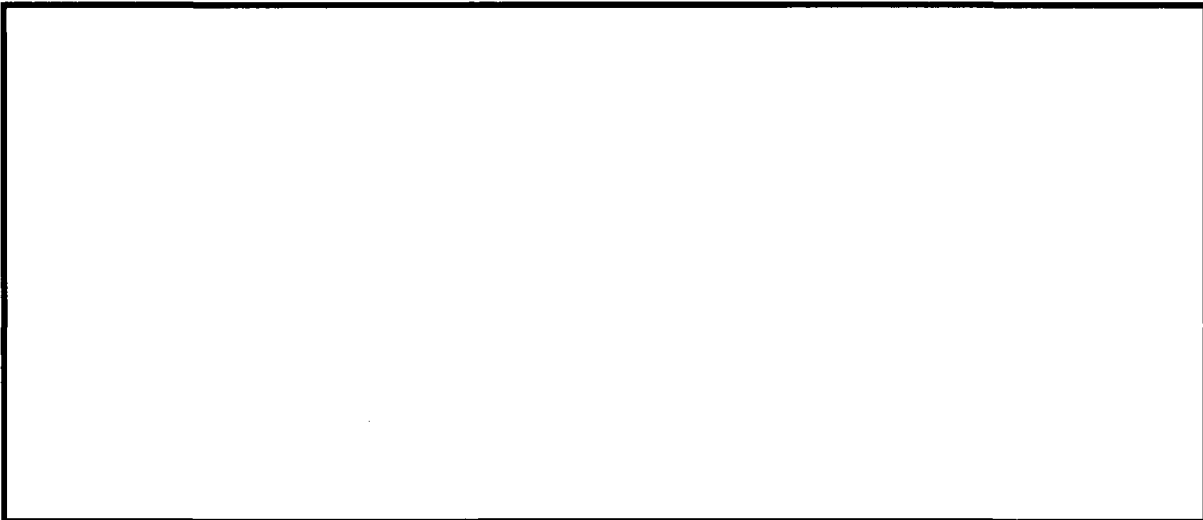
[Redacted]

b2
b7E

[Redacted]



b2
b7E



b2
b7E

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



7.2.1.1 Non-U.S. Citizens



7.2.2 Contingency Planning

7.2.2.1 System Backup

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Backup Program Procedures:

[Redacted]

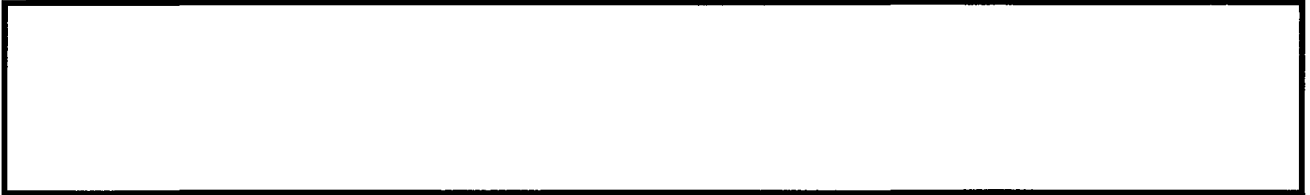
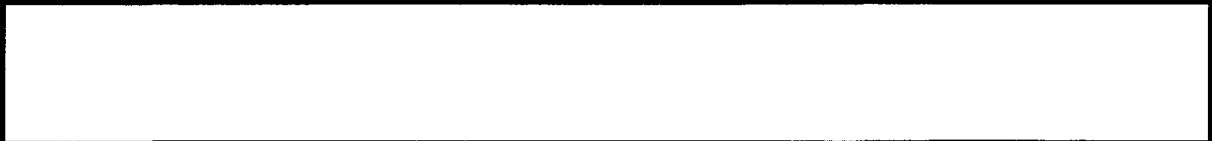
[Redacted]

[Redacted]



7.2.2.1.1 Backup Protection

b2
b7E

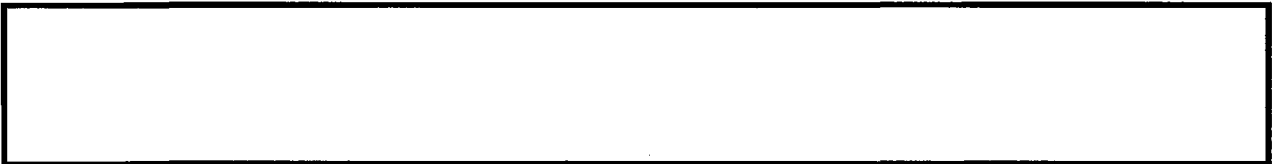


7.2.2.1.2 On-site & Off-site Storage



7.2.2.2 Telecommunications Services

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

[Redacted]

[Redacted]

[Redacted]

7.2.2.4.2 Disaster Recovery Plan

[Redacted]

b2
b7E

7.2.3 Configuration Management Program

[Redacted]

[Redacted]

Hardware:

[Redacted]

b2
b7E

Software:

[Redacted]

[Redacted]

Documentation:

[Redacted]

7.2.3.1 Hardware & Software Procurement

[Redacted]



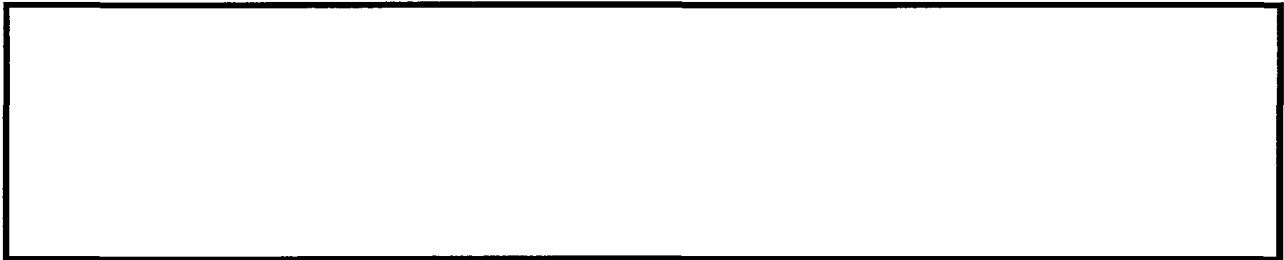
7.2.3.2 Evaluation



b2
b7E

7.2.4 Maintenance

7.2.4.1 Maintenance and Repair Procedures

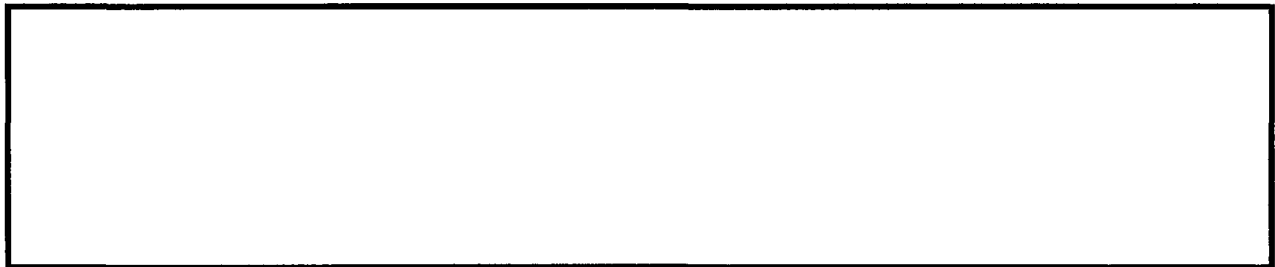


7.2.4.2 Maintenance Procedures Using Uncleared Personnel



b2
b7E

7.2.4.3 Maintenance Logs



7.2.4.4 Hardware & Software Maintenance

7.2.4.4.1 System Start-Up/Shut-Down

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b2
b7E

[Redacted]

[Redacted]

b2
b7E

[Redacted]

[Redacted]

7.2.4.4.2 Security Controls and Operations during Maintenance

[Redacted]

7.2.4.4.3 Remote Diagnostics

b2
b7E

[Redacted]

7.2.4.4.4 Hardware & Software Transfer, Relocation, and Release

[Redacted]

7.2.5 System & Information Integrity

7.2.5.1 System Integrity

7.2.5.1.1 System Start-up



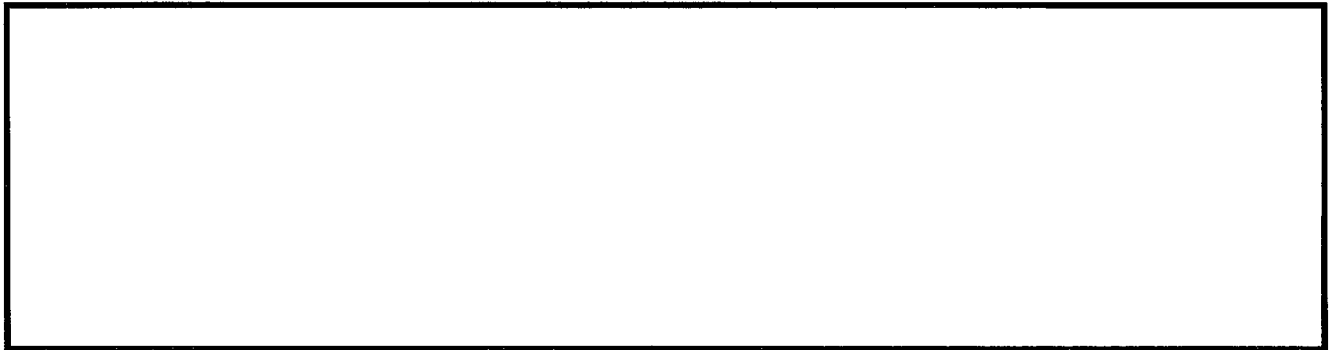
7.2.5.1.2 After Hours Processing Procedures



7.2.5.2 Data and Software Integrity

b2
b7E

7.2.5.2.1 Data and Software Integrity Procedures



b2
b7E

7.2.5.2.2 Data Copying, Reviewing, and Release Procedures



[Redacted]

[Redacted]

[Redacted]

b2
b7E

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.

b2
b7E

7.2.6 User's Guides

7.2.6.1 Configuration Guides

[Redacted]

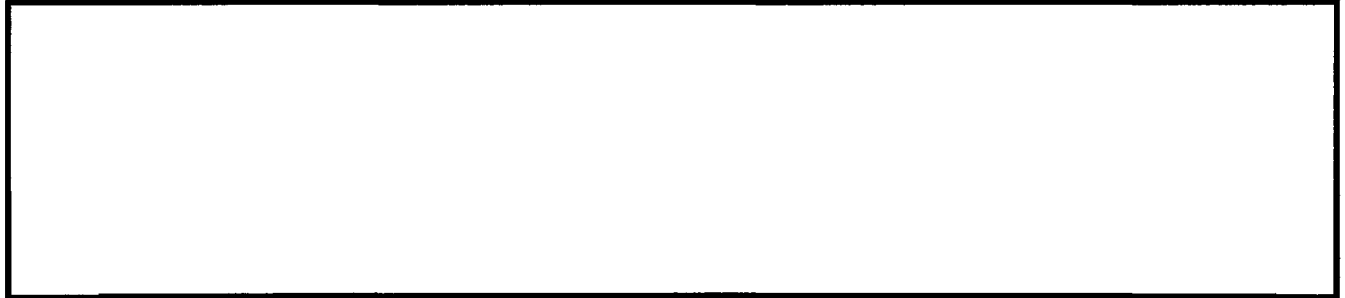
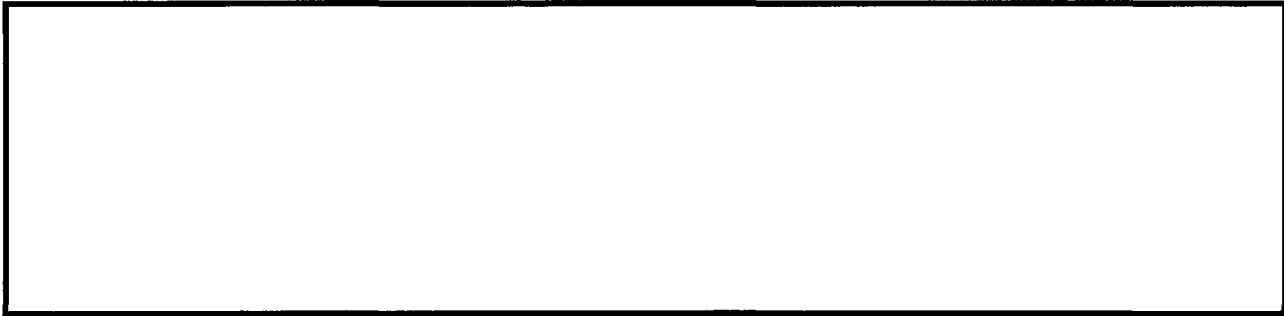
7.2.6.2 Guides for Privileged Users

Not applicable to the DCS 3000 system.

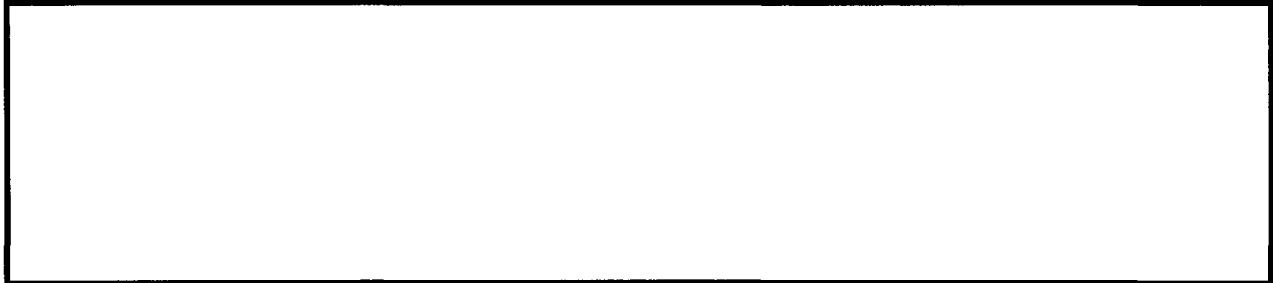
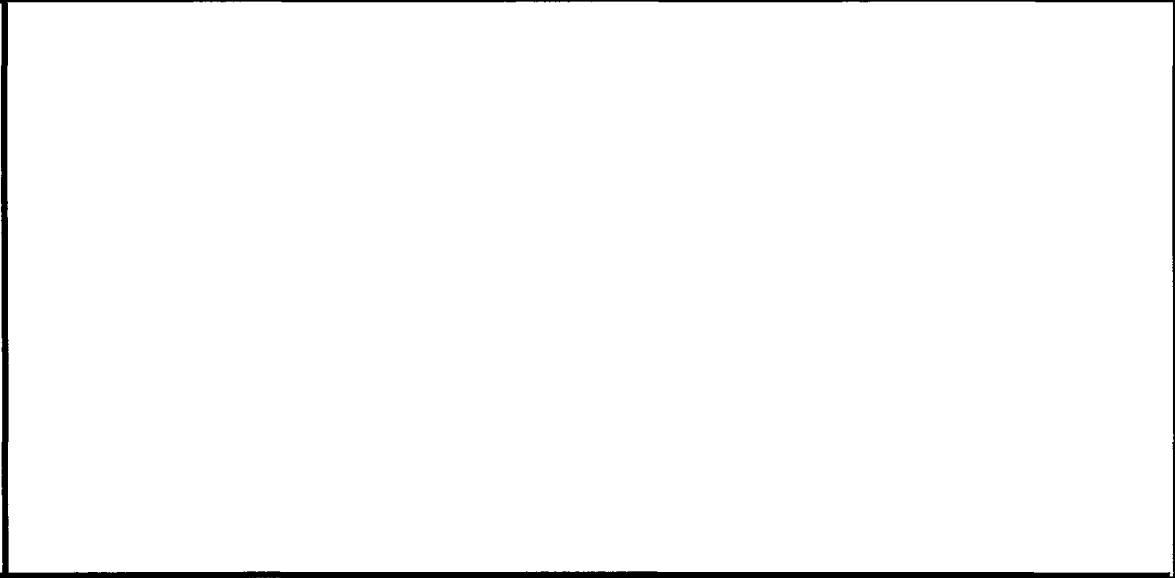
7.2.6.3 Guides for General Users

[Redacted]

7.2.7 Incident Response



b2
b7E



b2
b7E

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.

b2
b7E

7.3.1.2.1 Internal Marking

[Redacted]

7.3.1.3 Technical Access Control Mechanism

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b2
b7E

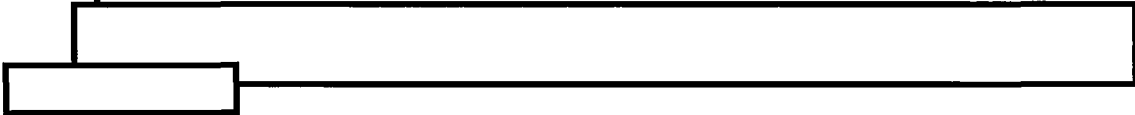
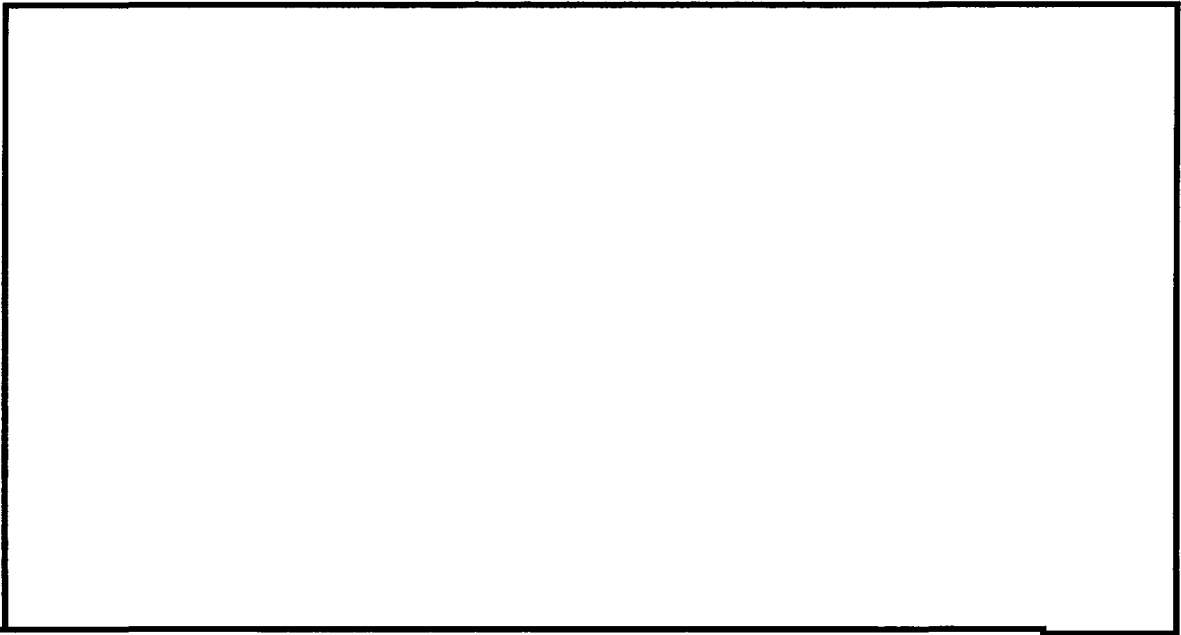
[Redacted]



7.3.1.4 User Group and Access Rights

7.3.1.4.1 User Groups

b2
b7E



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

b2
b7E

7.3.1.4.2.1 Local System Access Rights





7.3.1.4.2.2 Remote System Access



b2
b7E

7.3.1.4.2.3 Non-Data File Access



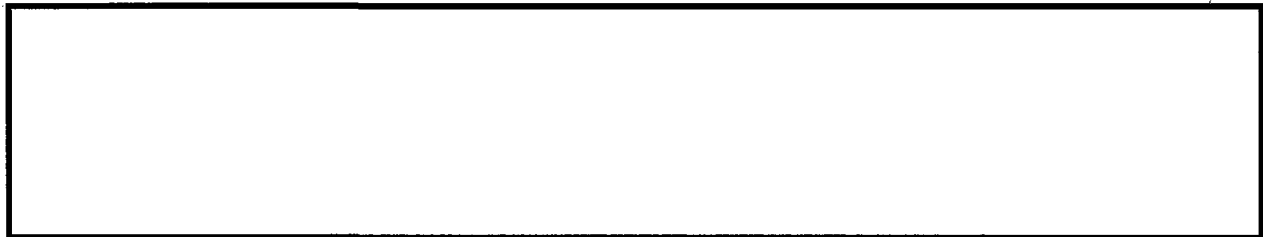
7.3.1.4.3 Privileged Users Access Rights



b2
b7E

7.3.1.5 Unsuccessful Logon Attempts

7.3.1.5.1 Log-on Error Handling





7.3.1.5.2 Account Lockout Handling



b2
b7E

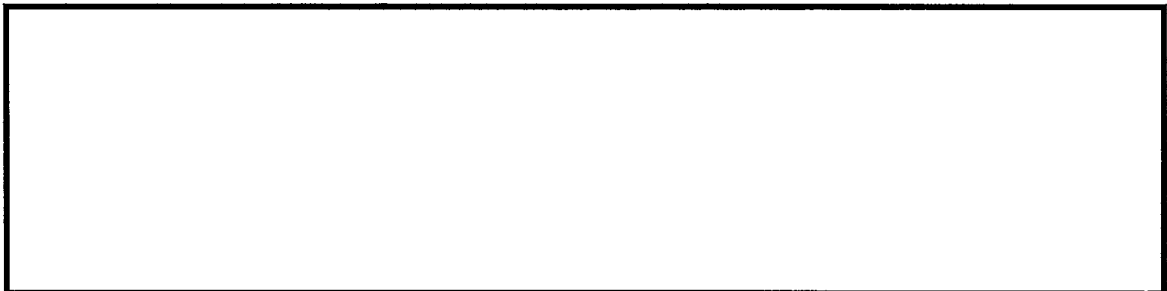
7.3.2 Identification & Authentication



7.3.2.1 System Users

b2
b7E

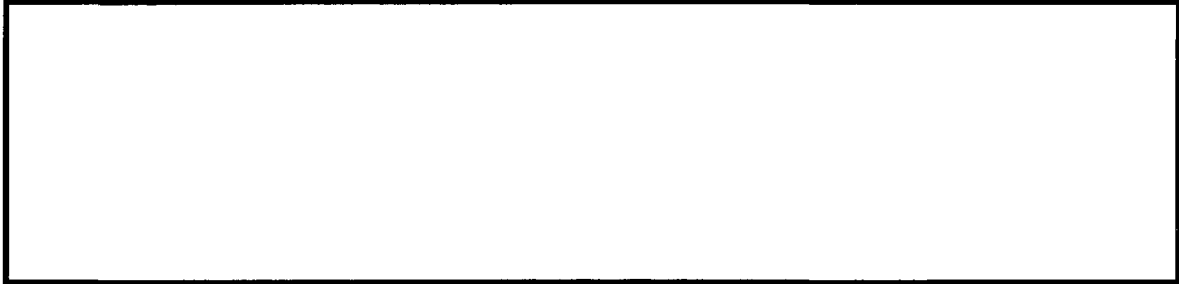
7.3.2.1.1 General Users





7.3.2.1.2 Privileged User

b2
b7E



7.3.2.1.3 Device/System User

Account Identifier	Account Privilege Level	Requirement Description
--------------------	-------------------------	-------------------------



7.3.2.2 Account Management Procedures

b2
b7E

7.3.2.2.1 Account Request Procedures



[Redacted]

7.3.2.2.2 Account Maintenance Procedures

[Redacted]

b2
b7E

7.3.2.2.3 Account Termination Procedures

[Redacted]

7.3.2.3 Authenticator Procedures

[Redacted]

[Redacted]

[Redacted]

b2
b7E

[Redacted]

7.3.2.3.1 Password Generation

[Redacted]

b2
b7E

[Redacted]

[Redacted]

7.3.2.3.2 Password Changes

b2
b7E

[Redacted]

[Redacted]

7.3.2.4 PKI Use

[Redacted]

7.3.3 Accountability (Including Audit Trails)

b2
b7E

7.3.3.1 Auditing Procedures

[Redacted]

[Redacted]

[Redacted]

7.3.3.1.1 Audit Review

[Redacted]

[Redacted]

[Redacted]

7.3.3.1.2 Audit Log Storage Requirements

b2
b7E

[Redacted]

[Redacted]

[Redacted]

7.3.3.1.3 Discrepancy Handling

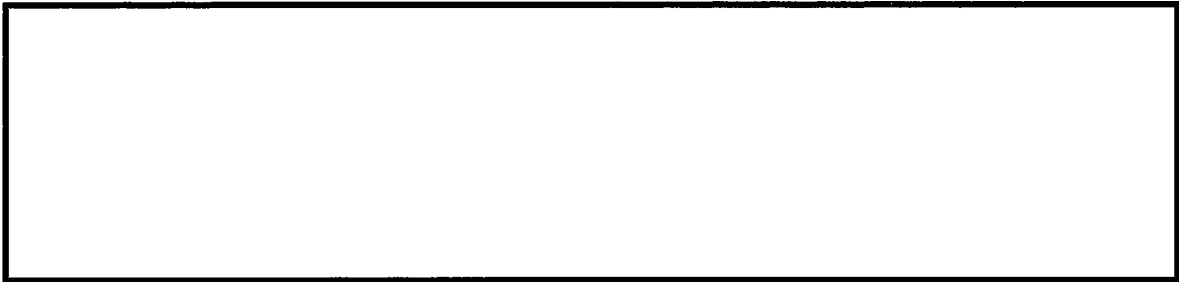
[Redacted]

b2
b7E

7.3.3.2 Notification Banner

[Redacted]

7.3.3.3 User Accountability



b2
b7E

7.3.3.4 Audit Protection and Log Access

7.3.3.4.1 Audit Protection



See section 7.3.3.4.2.

7.3.3.4.2 Audit Log Access



b2
b7E



7.3.3.5 Audited Information

7.3.3.5.1 Windows Operating System





7.3.3.6 Audited Activities

b2
b7E

7.3.3.6.1 Windows Operating System

Event Description	Success	Failure	Comment

FOR OFFICIAL USE ONLY

Event Description	Success	Failure	Comments
-------------------	---------	---------	----------

--	--	--	--

7.3.3.6.2 Other

--

b2
b7E

7.3.4 System & Communications Protection

7.3.4.1 System Protections

7.3.4.1.1 Malicious Code/Virus Protection

--

7.3.4.1.2 Denial of Service Protection

--

7.3.4.1.3 Priority Process Protection

Not applicable to the DCS 3000 system.

b2
b7E

7.3.4.2 Communications Protection

--

[Redacted]

7.3.4.2.1 Network Allowed Services and Protocols

7.3.4.2.1.1 Internal to the LAN:

SOURCE	DESTINATION	PROTOCOL	SERVICE
[Redacted]			

7.3.4.2.1.2 External to the LAN:

SOURCE	DESTINATION	PROTOCOL	SERVICE
[Redacted]			

7.3.4.2.2 Controlled Interface Requirements

[Redacted]

7.3.4.2.2.1 Controlled Interface to DCS 5000

b2
b7E

NOMENCLATURE	CONNECTED SYSTEM NAME	PURPOSE
[Redacted]		

7.3.4.2.2.2 Controlled Interface to DCS 6000

NOMENCLATURE	CONNECTED SYSTEM NAME	PURPOSE
[Redacted]		

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.

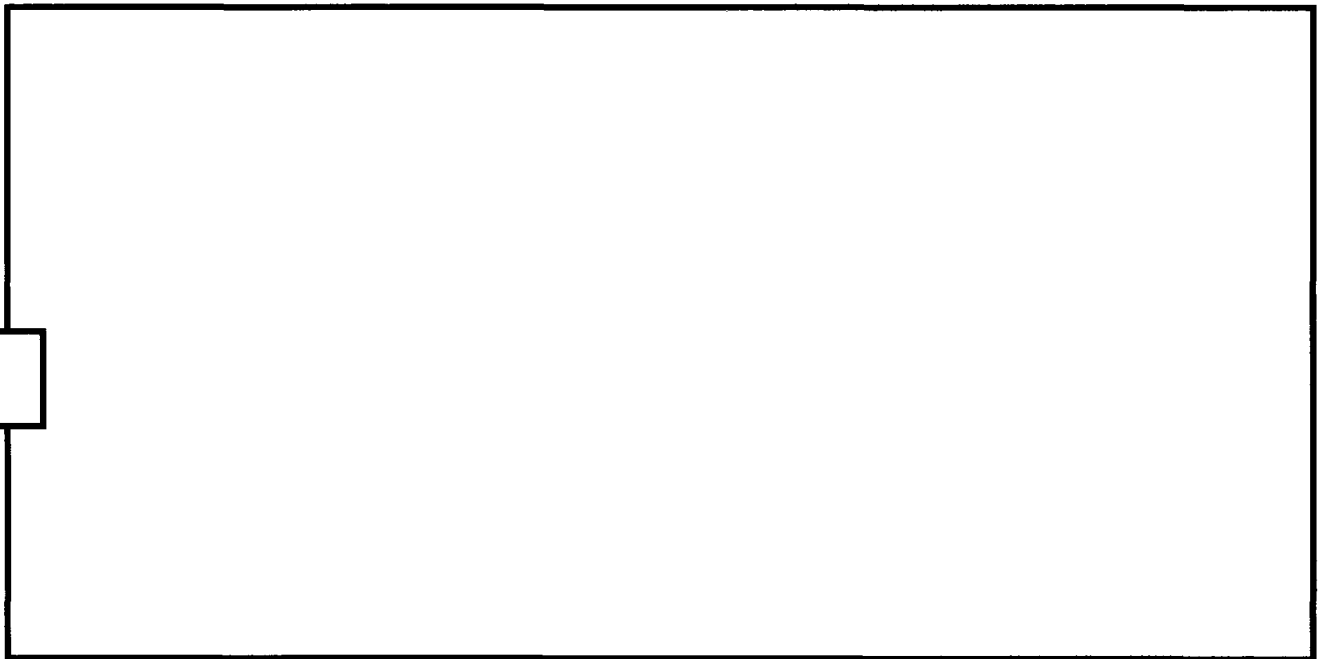
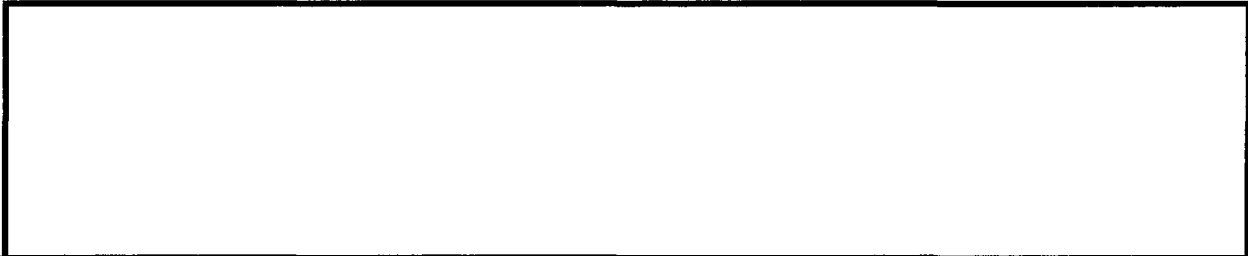
7.3.4.3.4 Wireless Devices

Not applicable to the DCS 3000 system.

8. SECURITY AWARENESS PROGRAM

b2
b7E

8.1 Program Description



b2
b7E



9. EXCEPTIONS

Not applicable to the DCS 3000 system.

10. GLOSSARY OF TERMS

<u>Acronym</u>	<u>Meaning</u>
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

FOR OFFICIAL USE ONLY

KVMKeyboard Video Mouse
LANLocal Area Network
LEALaw Enforcement Agency
LoCLevel of Concern
MACMandatory Access Control
MAOPManual of Administrative Operations and
Procedures
MbpsMegabits per second
MD5Message Digest Algorithm 5
MIOGManual of Investigative Operations and
Guidelines
MOAMemoranda of Agreement
MOUMemorandum of Understanding
N/ANot Applicable
NARANational Archives and Records Administration
O&MOperations and Maintenance
OTDOperational Technology Division
PKIPublic Key Infrastructure
PLProtection Level
PMProject Manager
PSIPersonnel Security Interview
RARisk Assessment
RMRisk Management
SACSpecial Agent in Charge
SAICSenior Special Agent in Charge
SBITSwitch Based Intercept Team
SCISensitive Compartmented Information
SCIFSensitive Compartmented Information Facility
SLAService Level Agreement
SSPSystem Security Plan
SSSSecurity Support Structure
TCPTransmission Control Protocol
TICTUTelecommunications Intercept and Collection
Technology Unit
TSPTelecommunications Service Provider
TTATechnically Trained Agent
UPSUninterruptible Power Supply
VPNVirtual Private Network
WANWide Area Network

FOR OFFICIAL USE ONLY

Attachments

Attachment A - Organizational Structure

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

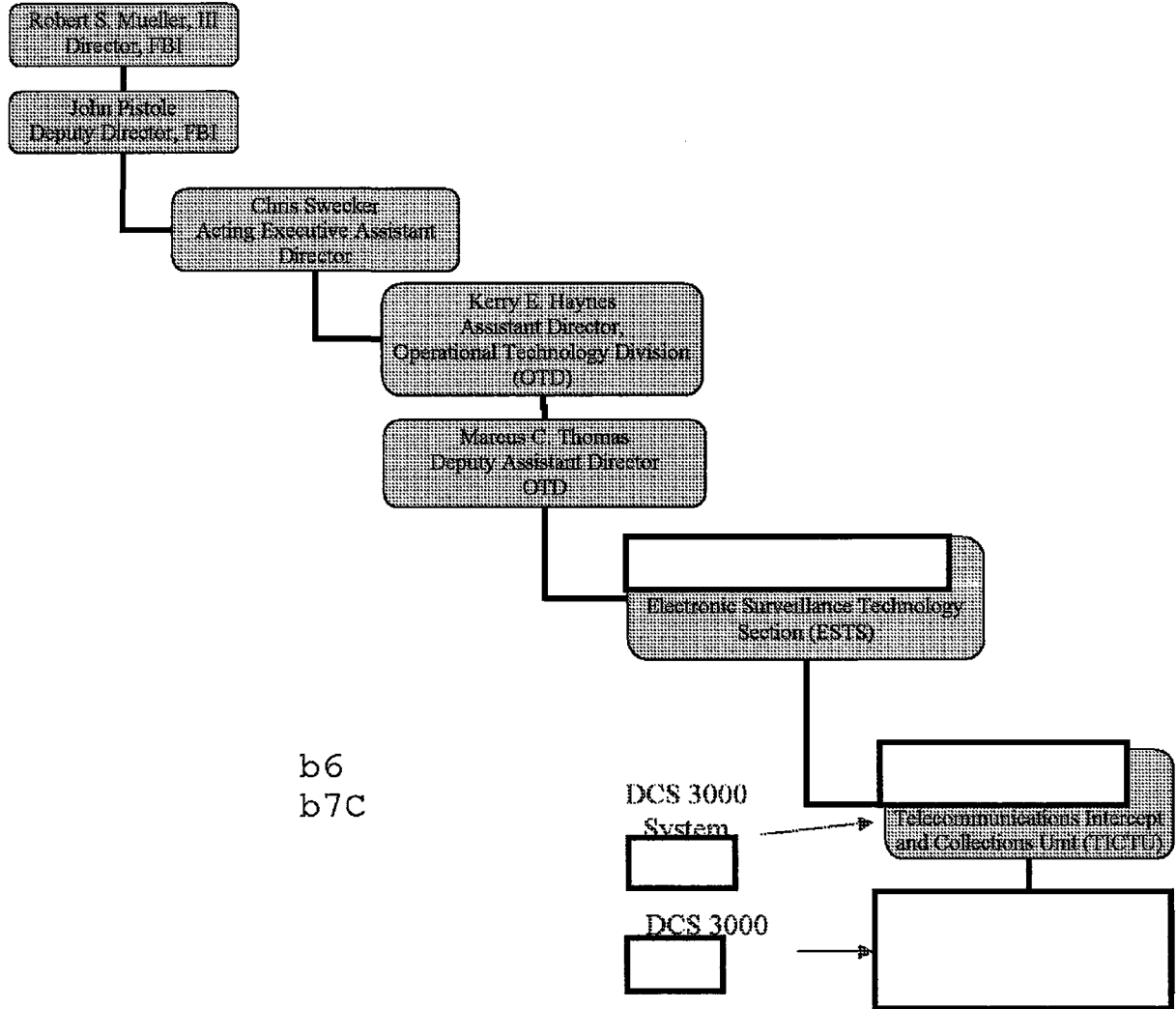
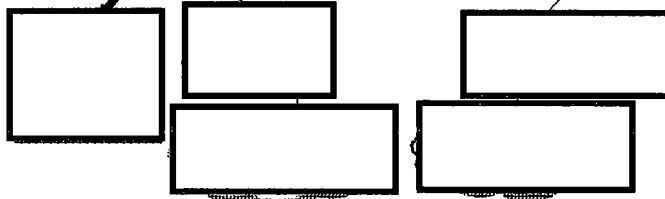
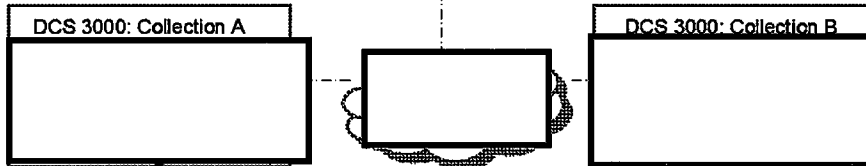


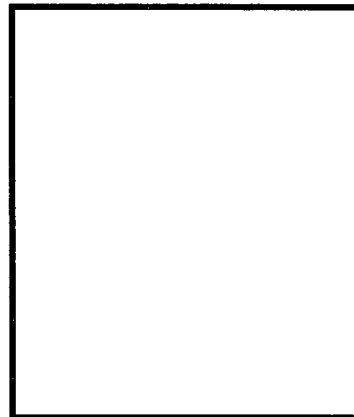
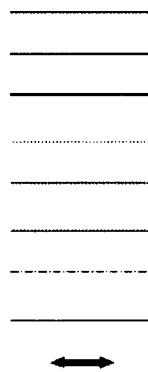
Figure 2: Organization Structure for DCS 3000 Program Management

Attachment B – Detailed System Diagram or System Security Architecture



b2
b7E

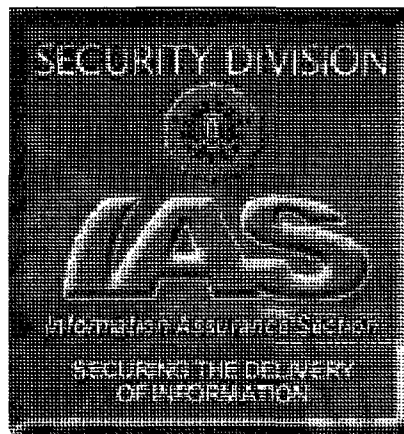
Legend



b2
b7E


Figure 3: Typical DCS 3000 Configuration

Executive Summary Validation of System Mitigation Actions Security Test Report



DCS3000

May 26, 2006


Certification Unit
Information Assurance Section
Security Division

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

INTRODUCTION

[Redacted]

b2
b7E

[Redacted]

[Redacted]

USE OF OPERATIONAL DATA & CONNECTIVITY REQUIREMENTS

[Redacted]

b2
b7E

SECURITY TESTING APPROACH

[Redacted]

TEST SUMMARY

[Redacted]

b2
b6
b7C
b7E



b2
b6
b7C
b7E

FINDINGS¹



b2
b7E

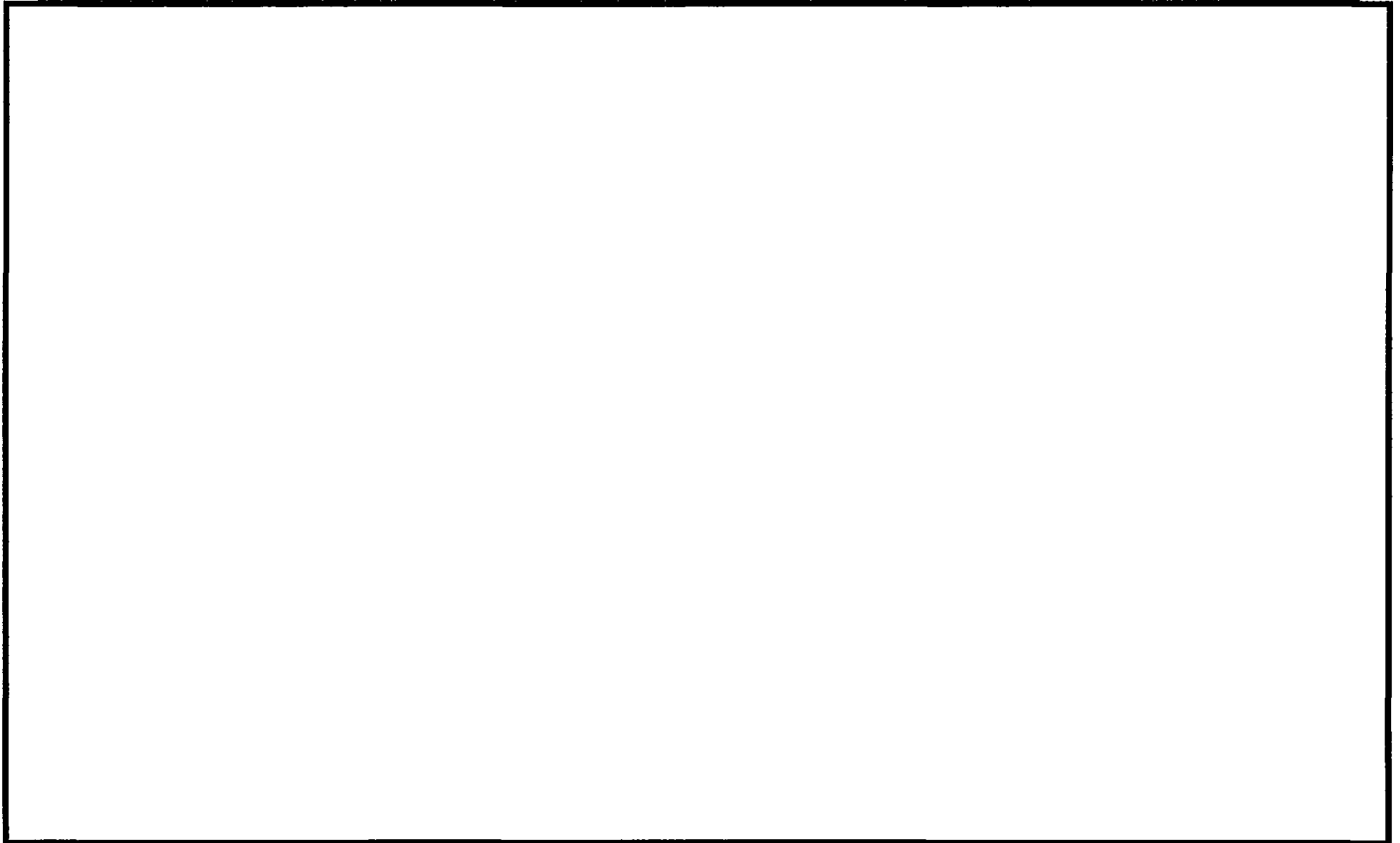
Table 1 – Validation Results

DCS3000 VALIDATION RESULTS			
Validation Area	DCS3000 Test Case	Minimum of Expected Results (per test case)	Actual Results

[Empty table body]			
--------------------	--	--	--

b2
b7E

DCS3000 VALIDATION RESULTS



b2
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/2/2006

To: Operational Technology

Attn: [Redacted]

Security

Attn: [Redacted]

From: Security

Information Assurance/Accreditation/SPY-B F-501

Contact: [Redacted]

202-[Redacted]

b6
b7C

Approved By: [Redacted]

Drafted By: [Redacted]

mlm

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

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

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

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

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

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

To: Operational Technology From: Security
Re: 319U-HQ-1487677-SECD, 05/2/2006

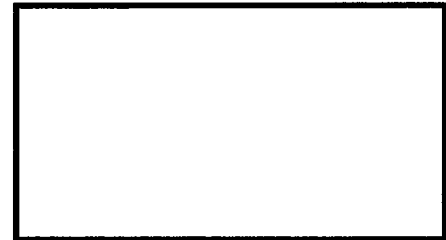
b2
b7E

The DCS-3000 application suite was developed to assist Law Enforcement Agencies (LEA) with collecting and processing data for court-ordered Electronic Surveillance (ELSUR) operations. The DCS-3000 collects [REDACTED]

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

The Certification and Accreditation Team Members are:

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



b6
b7C

To: Operational Technology From: Security
Re: 319U-HQ-1487677-SECD, 05/2/2006

LEAD(s) :

Set Lead 1: (Info)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

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

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

For information only.

CC:



b6
b7C

◆◆

LIMITED OFFICIAL USE ONLY



**System Security Plan (SSP)
Appendix D
DCS 3000 Pre-Certification System Vulnerability Assessment**

August 27, 2002

b6
b7C

Prepared by:
Certification Test Team



LIMITED OFFICIAL USE ONLY

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-29-2007 BY 65179 DMH/TAM/KSR/JB

LIMITED OFFICIAL USE ONLY

**System Security Plan (SSP)
DCS 3000
Pre-Certification Test Results and Findings**

(U) Table of Contents

1.0 PRE-CERTIFICATION TEST RESULTS F-1
 1.1 Testing Constraints F-1
 1.2 Major Findings F-2
 1.2.1 Technical Findings F-2
 1.2.2 Procedural/Policy Findings F-8

2.0 TEST SCHEDULE F-9

3.0 TECHNICAL TESTS AND TEST RESULTS F-10

BANNERS AND LABELS TEST SCRIPTS AND RESULTS F-11
 Test Case BL-01: Test for Standard Security Warning Banner F-11
 Test Case BL-02: Verifying Hardware has Proper Government Property Tags and Labeled with Proper Security Labels
 F-13
 Test Case BL-03: Verify Removable Media has Proper Security Labeling.
 Verify the existence of proper procedures for Disposal of hard Copy/Magnetic Media.
 Verify Backup Media Protection F-15
 Test Case BL-04: Data Record Marking F-17

SYSTEM INTEGRITY TEST SCRIPTS AND RESULTS F-18
 Test Case SI-01: Test for Anti-Virus Protection F-18

August 27, 2002

LIMITED OFFICIAL USE ONLY

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-01-2007 BY 65179 DMH/KSR/DK

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Test Case SI-02: Verifying System Data and Program Backup and Restore	F-20
Test Case SI-03: Verifying System Integrity Safeguards	F-24
Test Case SI-04: Verifying System Software Licenses	F-26
NETWORK CONNECTIVITY TEST SCRIPTS AND RESULTS	F-27
Test Case NC-01: Intranet Connectivity	F-27
Test Case NC-03: Verifying Physical Connections	F-30
NETWORK VULNERABILITY SCANNER TEST SCRIPTS AND RESULTS	F-31
Test Case NS-01: Identify network vulnerabilities using Cisco Security Scanner (CSS)	F-31
AUTOMATED VULNERABILITY SCANS AND RESULTS	F-35
Test Case VS-01: Determine System Vulnerabilities Using the Internet Security Systems (ISS) System Scanner	F-35
Test Case VS-03: Determine Windows Operating System Vulnerabilities Using the DISA Security Readiness Review Scripts	F-38
WINDOWS 2000 SYSTEM POLICIES	F-41
Test Case PS-W2K-01: Verify System Policies	F-41
WINDOWS 2000 IDENTIFICATION AND AUTHENTICATION TEST SCRIPTS AND RESULTS	F-53
Test Case IA-02: Test Password Requirement for System Access	F-53

August 27, 2002

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)
DCS 3000
Pre-Certification Test Results and Findings

1.0 PRE-CERTIFICATION TEST RESULTS

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

1.1 Testing Constraints

(U) [Redacted]

[Redacted]

August 27, 2002

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

b2
b7E

(U)

[Redacted]

1.2 Major Findings

(U)

[Redacted]

*****CAUTIONARY REMARK*****

(U)

[Redacted]

(U)

[Redacted]

b2
b7E

1.2.1 Technical Findings

(U)

~~(S)~~

[Redacted]

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)
DCS 3000
Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
DISA SRR OS Scan			
1. (U) <input checked="" type="checkbox"/>	[Redacted]		
2. (U) <input checked="" type="checkbox"/>	[Redacted]		
3. (U) <input checked="" type="checkbox"/>	[Redacted]		
4. (U) <input checked="" type="checkbox"/>	[Redacted]		
6. (U) <input checked="" type="checkbox"/>	[Redacted]		
	[Redacted]		

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
ISS System Scanner			
1(0) <input checked="" type="checkbox"/>			
			b2 b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
2. (U) <input checked="" type="checkbox"/>			
			b2 b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
3. (U) <input checked="" type="checkbox"/>			b2 b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
4(U) (S)	[Redacted]	[Redacted]	[Redacted] b2 b7E

(U) The following table briefly summarizes additional technical findings:

CISCO Secure Scanner			
1(U) (S)	[Redacted]	[Redacted]	[Redacted]
2(U) (S)	[Redacted]	[Redacted]	[Redacted]

August 27, 2002

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Operating System Manual Testing	
1. (U)	<input checked="" type="checkbox"/>

1.2.2 Procedural/Policy Findings

(U) [Redacted]
[Redacted]

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

b2
b7E

2.0 TEST SCHEDULE

(U)

[Redacted]

(U)

[Redacted]

(U)

Test Script And Result File	Testing Completed	Results Recorded	Analyses Completed
[Redacted]			



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

3.0 TECHNICAL TESTS AND TEST RESULTS

(U)

[Redacted]

(U)

[Redacted]

b2
b7E

(U)

[Redacted]

1)

(U)

[Redacted]

2)

(U)

[Redacted]

3)

(U)

[Redacted]

b2
b7E

4)

(U)

[Redacted]

BANNERS AND LABELS TEST SCRIPTS AND RESULTS

(U)

[Redacted]

(U)

[Redacted]

(U)

[Redacted]

[Redacted]

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

Requirement	Pass/Fail	Comment
<p>(U) MIOG 35-9.3.1(5)(b): The following banner shall be displayed on all FBI ADPT systems at a point prior to the user signing onto the 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 the appropriate officials."</p>	<p>Pass</p>	<p>b2 b7E</p>

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
------	-----------	------------------	-------------	----------------

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
------------	------------	------------	------------	------------

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
------------	------------	------------	------------	------------

(U) [Redacted]

Requirement	Pass/Fail	Comment
-------------	-----------	---------

[Redacted]	[Redacted]	[Redacted]
------------	------------	------------

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.13(1) : ADPT equipment and storage media that has processed FBI information may only be reused (e.g., transferred to another unit) within FBI control systems (i.e., formal access programs, SCIF, and TEMPEST) after they have been cleared by FBI employees. The microcomputer or ADPT storage media remains labeled and secured to the highest level of information ever entered into, stored on, or processed by the device.	Pass	
(U) DOJ 2640.2D 26.b . IT systems shall contain an external classification marking authorizing the level of information that can be processed.	Pass	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

[Redacted]

b2
b7E

(U)

[Redacted]

(U)

[Redacted]

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				

(U)

[Redacted]

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.10(1)(b): Removable media must be labeled with external markings. An exception to this policy is granted for computer center operations supporting a computerized tape management system that provides internal classification and data descriptor designations, as long as the media remains in FBI controlled space. However, all magnetic media leaving FBI controlled spaces must be labeled with the external classification and data descriptor labels.	[]	b2
(U) MIOG 35-9.4.14(1)(c): When inoperable diskettes tape cartridges printouts ribbons and similar items used to process sensitive or classified information must be destroyed in accordance with MIOG Part II Section 26.	[]	b7E
(U) MIOG 35-9.4.14(1)(d): When inoperable hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal following procedures provided in MIOG Part II Section 26.	[]	

August 27, 2002

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

(U) [Redacted]

b2
b7E

(U) [Redacted]

[Redacted]

(U) [Redacted]

(U) [Redacted]

Step	Procedure	Expected Outcomes	Date Tested	Actual Outcomes
[Redacted]				

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

b2

b7E

SYSTEM INTEGRITY TEST SCRIPTS AND RESULTS

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

b2
b7E

System Security Plan (SSP)
DCS 3000
Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

b2
b7E

(U)

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.4(4): Whenever a virus infection is detected, it should be reported to the ADPT Security Officer.	Fail	Presently, there are no virus checking programs in place
(U) MIOG 35-9.4.5(4): Vendor diagnostic software must be scanned, write-protected, and retained by the Computer Specialist. Only this copy of the software may be used on FBI ADPT systems.	Fail	Presently, there are no virus checking programs in place
(U) DOJ 2640.2D 10. Components shall establish procedures to ensure that computer software installed on component IT systems is in compliance with applicable copyright laws and is incorporated into the system's life cycle management process.	Fail	Presently, there are no virus checking programs in place
(U) DCID 6/3 MalCode: Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).	Fail	Presently, there are no virus checking programs in place

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

b2

b7E

(U)

[Redacted]

[Redacted]

[Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

b2
b7E

b6
b7C

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

Requirement	Pass/Fail	Comment
<p>(U) MIOG 35-8.1.2(3): System security plan documentation is required for every classified and sensitive FBI ADPT system. The components of a system security plan are:</p> <ul style="list-style-type: none"> a) system security plan following OMB 90-08 or its successor b) documented risk management actions pertaining to the ADPT system c) certification statement that reflects the results of certification tests of the security features applicable to the system d) contingency plan which consists of an emergency response plan, backup operations plan, and post-disaster recovery plan e) standard security procedures for users and operators of the system. 	<p>Pass</p>	
<p>DCID 6/3 Doc 1: Documentation shall include:</p> <ul style="list-style-type: none"> A System Security Plan. A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern. 	<p>Pass</p>	
<p>DCID 6/3 Doc2: Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.</p>	<p>Pass</p>	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
<p>DCID 6/3 Doc3: The DAA may direct that documentation also shall include:</p> <p>Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.</p> <p>Reports of test results.</p> <p>A general user's guide that describes the protection mechanisms provided and that supplies guidelines on how the mechanisms are to be used and how they interact.</p>	<p>Pass</p>	
<p>DCID 6/3 Verif2: Verification by the DAA Rep that the necessary security procedures and mechanisms are in place; testing of them by the DAA Rep to ensure that they work appropriately.</p>	<p>N/A</p>	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
<p>(U) DOJ 2640.2D 9.1. [Components shall:] Develop a contingency plan for each general support system and major application. Contingency plans shall:</p> <p>(1) Identify the priorities of the system for restoration, taking into consideration the system's role in fulfilling Department mission and interdependency requirements.</p> <p>(2) Determine the maximum amount of elapsed time permissible between an adverse event and putting the system's contingency plan into operation.</p> <p>(3) Determine the maximum amount of data and system settings that can be lost between the service interruption event and the last back-up (this measure shall determine system back-up policies).</p> <p>(4) Identify interdependencies with other systems (i.e., other component, Federal, State or local agencies) that could affect contingency operations.</p> <p>(5) Identify system owners, roles, and responsibilities.</p>	Pass	
<p>(U) DOJ 2640.2D 9.2. [Components shall:] Develop and maintain site plans that detail responses to emergencies for IT facilities.</p>	Pass	
<p>(U) DOJ 2640.2D 9.3. [Components shall:] Test contingency/business resumption plans annually or as soon as possible after a significant change to the environment, that would alter the in-place assessed risk.</p>	Pass	
<p>(U) MIOG 35-9.4.4(3): Executable software authorized to run on an FBI ADPT system shall be identified in the system security plan. The level of protection must be commensurate with the sensitivity of the information processed. At a minimum, such media should be backed up and stored physically separated from the system or at an off-site location.</p>	Pass	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) [Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

b2
b7E

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				

(U) Pass/Fail:

Requirement	Pass/Fail	Comment
MIOG 35-9.4.4(3): requires that safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction of an ADPT system's application software, operating system software, and critical data files. The safeguards should achieve the integrity objectives and should be documented in the system security plan.	Pass	
DOJ 2640.2D 8. Component IT systems shall be examined for security prior to being placed into operation. All IT systems shall have safeguards in place to detect and minimize inadvertent or malicious modifications or destruction of the IT system.	Pass	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
DCID 6/3 Integrity2: Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g., integrity locks, encryption).	Pass	
DCID 6/3 Integrity3: Integrity, including the implementation of specific non-repudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.	N/A	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) [Redacted] b2
 (U) [Redacted] b7E
 (U) [Redacted]
 (U) [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				

(U) [Redacted]

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.4(5): Use of software shall comply with copyright laws.	Pass	
(U) MIOG 35-9.4.5(4): Vendor diagnostic software must be scanned, write-protected, and retained by the Computer Specialist. Only this copy of the software may be used on FBI ADPT systems.	Pass	
(U) DOJ 2640.2D 10. Components shall establish procedures to ensure that computer software installed on component IT systems is in compliance with applicable copyright laws and is incorporated into the system's life cycle management process.	Pass	

NETWORK CONNECTIVITY TEST SCRIPTS AND RESULTS

b2
b7E

(U) [Redacted]
(U) [Redacted]
[Redacted]
[Redacted]
(U) [Redacted]
[Redacted]
(U) [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				
[Redacted]				

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Status	Procedure	Expected Outcome	Data Received	Actual Outcome
[Redacted Content]				
[Redacted Content]				

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

U

Requirement	Pass/Fail	Comment
MIOG 35-6(4) Connectivity is prohibited between internal FBI ADPT systems and all other systems or networks not covered under the FBI's management authority without approval of the FBI accrediting authority.	N/A	
MIOG 35-9.3.1(6) Interconnections between sensitive and classified FBI ADPT systems and non-FBI ADPT systems must be established through controlled interfaces. The ADPT Security Officer must be consulted for guidance on establishing controlled interfaces. The controlled interfaces used in an ADPT system implemented as a network shall be accredited at the highest classification level and most restrictive classification category of information on the network.	N/A	

b2
b7E

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

b2
b7E

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				
[Redacted]				

(U) [Redacted]

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.7: The ISAs and POCs must be able to identify all equipment processing storing or transmitting classified information whether operating as part of a network or in a standalone mode of operation. This requirement is in addition to the hardware and software inventory requirements stated in MIOG Part II Section 16-18.9.	Pass	

b2
b7E

NETWORK VULNERABILITY SCANNER TEST SCRIPTS AND RESULTS

(U) [Redacted]
(U) [Redacted]

August 27, 2002

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

[Redacted]

(U) [Redacted]

(U) [Redacted]

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(?)

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

b2
b7E



System Security Plan (SSP)

DCS 3000

b2

Pre-Certification Test Results and Findings

b7E

(?)

(?)

Requirement	Pass/Fail	Comment
(U) DOJ 2640.2D 16.e. [Access controls shall be in place and operational for all Department IT systems to:] Enforce separation of duties based on roles and responsibilities.	Pass	
(U) DOJ 2640.2D 16.f. [Access controls shall be in place and operational for all Department IT systems to:] Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure.	Fail	Telnet login in the clear and address cited in the router and access list.
(U) DOJ 2640.2D 16.g. [Access controls shall be in place and operational for all Department IT systems to:] For systems operating in the system high mode of operation, the system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has a need-to-know.	Pass	

AUTOMATED VULNERABILITY SCANS AND RESULTS

b2
b7E

(U) [Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) ~~(S)~~

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

(U)

Requirement	Pass/Fail	Comment
(U) DOJ 2640.2D 7.h. Accreditations with conditions shall not be granted if system or application vulnerabilities permit the following: (1) Breaches to the confidentiality and integrity functions of the system or application and its data.	Pass	
(U) DOJ 2640.2D 16.e. [Access controls shall be in place and operational for all Department IT systems to:] Enforce separation of duties based on roles and responsibilities.	Pass	
(U) DOJ 2640.2D 16.f. [Access controls shall be in place and operational for all Department IT systems to:] Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure.	Pass	
(U) DOJ 2640.2D 16.g. [Access controls shall be in place and operational for all Department IT systems to:] For systems operating in the system high mode of operation, the system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has a need-to-know.	Pass	

August 27, 2002



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
<p>(U) MIOG 35-9.3.1(1): Prior to March 6, 2000, ADPT systems used for the processing of classified or sensitive information in the System High Security mode of operation must have the functionality of the C2 level of trust defined in the Department of Defense (DoD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center Technical Guide 005 (NSC-TG-005), provided guidance on achieving C2 functionality in a network. On October 8, 1999, the National Security Agency issued the "Controlled Access Protection Profile (CAPP)" to replace the C2 standard. All future procurements of DOJ computer systems operating in System High Security Mode MUST meet CAPP security requirements from the above date forward.</p>	Pass	
<p>(U) MIOG 35-9.3.1(4)(e): Access Control: For systems operating in the Systems High Security Mode of Operation, access control may be implemented through discretionary access control techniques through measures such as file passwords, access control lists, disk encryption or other techniques, as defined in the approved system security plan.</p>	Pass	



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

b2
b7E

(U) ~~X~~ [Redacted]

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
[Redacted]				

(U) ~~X~~ [Redacted]

(U) ~~X~~ [Redacted]

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(U) DOJ 2640.2D 16.a. [Access controls shall be in place and operational for all Department IT systems to:] Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more.	Pass	
(U) DOJ 2640.2D 16.e. [Access controls shall be in place and operational for all Department IT systems to:] Enforce separation of duties based on roles and responsibilities.	Pass	
(U) DOJ 2640.2D 16.f. [Access controls shall be in place and operational for all Department IT systems to:] Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure.	Pass	
(U) DOJ 2640.2D 16.g. [Access controls shall be in place and operational for all Department IT systems to:] For systems operating in the system high mode of operation, the system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has a need-to-know.	Pass	



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
<p>(U) MIOG 35-9.3.1(1): Prior to March 6, 2000, ADPT systems used for the processing of classified or sensitive information in the System High Security mode of operation must have the functionality of the C2 level of trust defined in the Department of Defense (DoD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center Technical Guide 005 (NSC-TG-005), provided guidance on achieving C2 functionality in a network. On October 8, 1999, the National Security Agency issued the "Controlled Access Protection Profile (CAPP)" to replace the C2 standard. All future procurements of DOJ computer systems operating in System High Security Mode MUST meet CAPP security requirements from the above date forward.</p>	Pass	
<p>(U) MIOG 35-9.3.1(4)(e): Access Control: For systems operating in the Systems High Security Mode of Operation, access control may be implemented through discretionary access control techniques through measures such as file passwords, access control lists, disk encryption or other techniques, as defined in the approved system security plan.</p>	Pass	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

WINDOWS 2000 SYSTEM POLICIES

(U) [Redacted]

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

b2
b7E

Pre-Certification Test Results and Findings

(U)

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome
------	-----------	-------------	--------------	------------------	----------------

August 27, 2002

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

August 27, 2002

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

August 27, 2002

System Security Plan (SSP)
DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome



b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

August 27, 2002

LIMITED OFFICIAL USE ONLY

F-50

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) ~~S~~

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.3.1(4)(a): User Identification: The ADPT system shall control and limit user access based on identification and authentication of the user. The identity of each user will be established positively before authorizing access. User identification and password systems support the minimum requirements of access control, least privilege, and system integrity.	Pass	
(U) MIOG 35-9.3.1(4)(b): Authentication: For ADPT systems requiring authentication controls the ADPT system shall ensure that each user of the ADPT system is authenticated before access is permitted. Currently use of a password system is the preferred method for authenticating users of FBI ADPT systems. More sophisticated authentication techniques such as retina scanners or voice recognition systems must be cost-justified through the risk analysis process. If passwords are selected as the authentication mechanism passwords will be authenticated each time they are used. FIPS PUB 83 provides standards for authentication.	Fail	Password restrictions are lacking.

b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
<p>(U) MIOG 35-9.3.1(4)(e): Access Control - For systems operating in the System High Security Mode of Operation, this may be implemented with discretionary access control techniques; through measures such as file passwords, access control lists, disk encryption or other techniques, as defined in the approved system security plan. For ADPT systems operating in the compartmented or multilevel security mode, mandatory access control (MAC) is required. MAC is a means of restricting access to information based on labels. A user's label indicates what information the user is permitted to access and the type of access (e.g., read or write) that the user is allowed to perform. An object's label indicates the sensitivity of the information that the object contains. A user's label must meet specific criteria defined by MAC policy in order for the user to be permitted access to a labeled object. This type of access control is always enforced above any discretionary controls implemented by users. Printed: 01/16/96.</p>	<p>Pass</p>	
<p>(U) MIOG 35-9.4.2(2)(d): User accounts that have been inactive for over 90 days will be suspended. The person responsible for administering the access control mechanism is authorized to reinstate such accounts up to 180 days overall. User accounts that have been inactive for 180 days will be deleted and may only be reissued by the person authorized to approve access who is identified in the access control criteria and only to an individual who has been authorized access.</p>	<p>Pass</p>	
<p>(U) DOJ 2640.2D 18.a. [Department IT systems that use passwords as the means for authentication shall implement at least the following minimum features:] Require the system administrator to issue initial passwords.</p>	<p>Pass</p>	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(U) DOJ 2640.2D 18.b [Department IT systems that use passwords as the means for authentication shall implement at least the following minimum features:] Require technical implementation to support the following: (1) An eight-character password composed of at least three of the following, English uppercase, English lower case, numerics, special characters.	Fail	
(2) Prevent the use of the previous six passwords.	Fail	
(3) Prevent the display of a clear text password.	Pass	
(4) Limit password lifetime to a maximum of 90 days.	Pass	
(5) Expire an initial use password at the time of its first use in a manner that requires the password owner to supply a new password.	Fail	
(U) DOJ 2640.2D 18.g. [Department IT systems that use passwords as the means for authentication shall implement at least the following minimum features:] Disable user accounts after no more than four consecutive invalid attempts are made to supply a password, and require the reinstatement of a disabled user account by an administrator.	Pass	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

WINDOWS 2000 IDENTIFICATION AND AUTHENTICATION TEST SCRIPTS AND RESULTS

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

[Redacted]

b2
b7E

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome

(U)

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

Requirement	Pass/Fail	Comment
DOJ 2640.2D 17.c. [Department systems shall:] Comply with the Department password management policy.	Fail	Does not comply with DOJ standards.
DOJ 2640.2D 18.b. [Department IT systems that use passwords as the means for authentication shall implement at least the following minimum features:] Require technical implementation to support the following: (1) An eight-character password composed of at least three of the following, English uppercase, English lower case, numeric, special characters. (2) Prevent the use of the previous six passwords. (3) Prevent the display of a clear text password. (4) Limit password lifetime to a maximum of 90 days. (5) Expire an initial use password at the time of its first use in a manner that requires the password owner to supply a new password.	Fail	Password does not expire (e.g. DCSgod).

b2
b7E

August 27, 2002

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: Immediate

Date: 05/31/2006

To: Security

Attn: [Redacted]
[Redacted]

From: Security

Information Assurance Section/Certification/SPY-B F-601

Contact: [Redacted] (202) [Redacted]

Approved By: [Redacted]

Drafted By: [Redacted]

cjp

Case ID #: 319U-HQ-1487677-SECD-300

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

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

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

Administrative: Additional References:

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

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

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

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

To: Security From: Security
Re: 319U-HQ-1487677-SECD 05/31/2006

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

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

b2
b7E

To: Security From: Security
Re: 319U-HQ-1487677-SECD 05/31/2006

LEAD(s) :

Set Lead 1: (Action)

SECURITY

AT WASHINGTON, DC

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

Set Lead 2: (Info)

SECURITY

AT WASHINGTON, DC

Attn: ISSM, [REDACTED] for your information.

CC:

[REDACTED]

b6
b7C