

*Freedom of Information
and
Privacy Acts*

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CD'S

Section: 9



Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 107

Page 159 ~ Duplicate Duplicate found Division CD's section 1
Page 160 ~ Duplicate Duplicate found Division CD's section 1
Page 161 ~ Duplicate Duplicate found Division CD's section 1
Page 162 ~ Duplicate Duplicate found Division CD's section 1
Page 163 ~ Duplicate Duplicate found Division CD's section 1
Page 164 ~ Duplicate Duplicate found Division CD's section 1
Page 165 ~ Duplicate Duplicate found Division CD's section 1
Page 166 ~ Duplicate Duplicate found Division CD's section 1
Page 167 ~ Duplicate Duplicate found Division CD's section 1
Page 168 ~ Duplicate Duplicate found Division CD's section 1
Page 169 ~ Duplicate Duplicate found Division CD's section 1
Page 170 ~ Duplicate Duplicate found Division CD's section 1
Page 171 ~ Duplicate Duplicate found Division CD's section 1
Page 172 ~ Duplicate Duplicate found Division CD's section 1
Page 173 ~ Duplicate Duplicate found Division CD's section 1
Page 174 ~ Duplicate Duplicate found Division CD's section 1
Page 175 ~ Duplicate Duplicate found Division CD's section 1
Page 176 ~ Duplicate Duplicate found Division CD's section 1
Page 177 ~ Duplicate Duplicate found Division CD's section 1
Page 178 ~ Duplicate Duplicate found Division CD's section 1
Page 179 ~ Duplicate Duplicate found Division CD's section 1
Page 180 ~ Duplicate Duplicate found Division CD's section 1
Page 181 ~ Duplicate Duplicate found Division CD's section 1
Page 182 ~ Duplicate Duplicate found Division CD's section 1
Page 183 ~ Duplicate Duplicate found Division CD's section 1
Page 184 ~ Duplicate Duplicate found Division CD's section 1
Page 185 ~ Duplicate Duplicate found Division CD's section 1
Page 186 ~ Duplicate Duplicate found Division CD's section 1
Page 187 ~ Duplicate Duplicate found Division CD's section 1
Page 188 ~ Duplicate Duplicate found Division CD's section 1
Page 189 ~ Duplicate Duplicate found Division CD's section 1
Page 190 ~ Duplicate Duplicate found Division CD's section 1
Page 191 ~ Duplicate Duplicate found Division CD's section 1
Page 192 ~ Duplicate Duplicate found Division CD's section 1
Page 193 ~ Duplicate Duplicate found Division CD's section 1
Page 194 ~ Duplicate Duplicate found Division CD's section 1
Page 195 ~ Duplicate Duplicate found Division CD's section 1
Page 196 ~ Duplicate Duplicate found Division CD's section 1
Page 197 ~ Duplicate Duplicate found Division CD's section 1
Page 198 ~ Duplicate Duplicate found Division CD's section 1
Page 199 ~ Duplicate Duplicate found Division CD's section 1
Page 200 ~ Duplicate Duplicate found Division CD's section 1
Page 201 ~ Duplicate Duplicate found Division CD's section 1
Page 202 ~ Duplicate Duplicate found Division CD's section 1

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

Page 203 ~ Duplicate Duplicate found Division CD's section 1
 Page 204 ~ Duplicate Duplicate found Division CD's section 1
 Page 205 ~ Duplicate Duplicate found Division CD's section 1
 Page 206 ~ Duplicate Duplicate found Division CD's section 1
 Page 207 ~ Duplicate Duplicate found Division CD's section 1
 Page 208 ~ Duplicate Duplicate found Division CD's section 1
 Page 209 ~ Duplicate Duplicate found Division CD's section 1
 Page 210 ~ Duplicate Duplicate found Division CD's section 1
 Page 211 ~ Duplicate Duplicate found Division CD's section 1
 Page 212 ~ Duplicate Duplicate found Division CD's section 1
 Page 213 ~ Duplicate Duplicate found Division CD's section 1
 Page 214 ~ Duplicate Duplicate found Division CD's section 1
 Page 215 ~ Duplicate Duplicate found Division CD's section 1
 Page 216 ~ Duplicate Duplicate found Division CD's section 1
 Page 217 ~ Duplicate Duplicate found Division CD's section 1
 Page 218 ~ Duplicate Duplicate found Division CD's section 1
 Page 219 ~ Duplicate Duplicate found Division CD's section 1
 Page 220 ~ Duplicate Duplicate found Division CD's section 1
 Page 253 ~ b5, b6, b7C
 Page 254 ~ b5
 Page 255 ~ b5
 Page 256 ~ b5
 Page 257 ~ b5, b6, b7C
 Page 258 ~ b2, b5, b7E
 Page 259 ~ b2, b5, b7E
 Page 260 ~ b2, b5, b7E
 Page 261 ~ b2, b5, b7E
 Page 262 ~ b5
 Page 263 ~ b5
 Page 264 ~ b5
 Page 265 ~ b5
 Page 266 ~ b5
 Page 267 ~ b5
 Page 268 ~ b5
 Page 269 ~ b5
 Page 270 ~ b5
 Page 271 ~ b5
 Page 272 ~ b5
 Page 273 ~ b5
 Page 274 ~ b2, b5, b7E
 Page 275 ~ b5
 Page 276 ~ b5
 Page 277 ~ b5
 Page 278 ~ b5

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

Page 279 ~ b2, b5, b7E
Page 280 ~ b2, b5, b7E
Page 281 ~ b5
Page 282 ~ b5
Page 283 ~ b5
Page 284 ~ b5
Page 285 ~ b5
Page 286 ~ b5
Page 287 ~ b5
Page 288 ~ b5
Page 289 ~ b2, b5, b7E
Page 290 ~ b5
Page 291 ~ b5
Page 292 ~ b5
Page 293 ~ b5
Page 294 ~ b5
Page 295 ~ b5
Page 296 ~ b5
Page 297 ~ b5

XXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXX

1 CI-100 DCS 3000 to EDMS SETUP MANUAL

1.1 Purpose and Scope

This document is designed to guide the System Administrator (SA) as well as the Information System Security Officer (ISSO) in the process of installing and configuring the hardware and software associated with properly setting up the CI-100 DCS 3000 to EDMS transfer. This document can, and should be used in conjunction with the contingency plan in the event the System Owner(s) find(s) is necessary to rebuild this portion of the system.

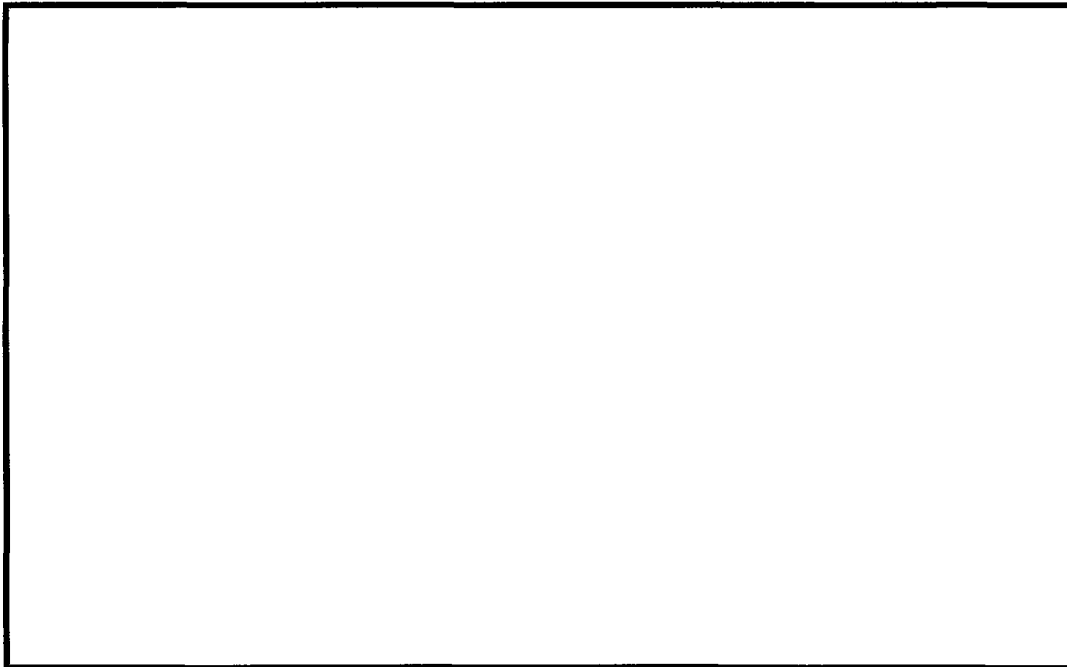
2 System Installation, Configuration, and Operation

2.1 Installation and Configuration

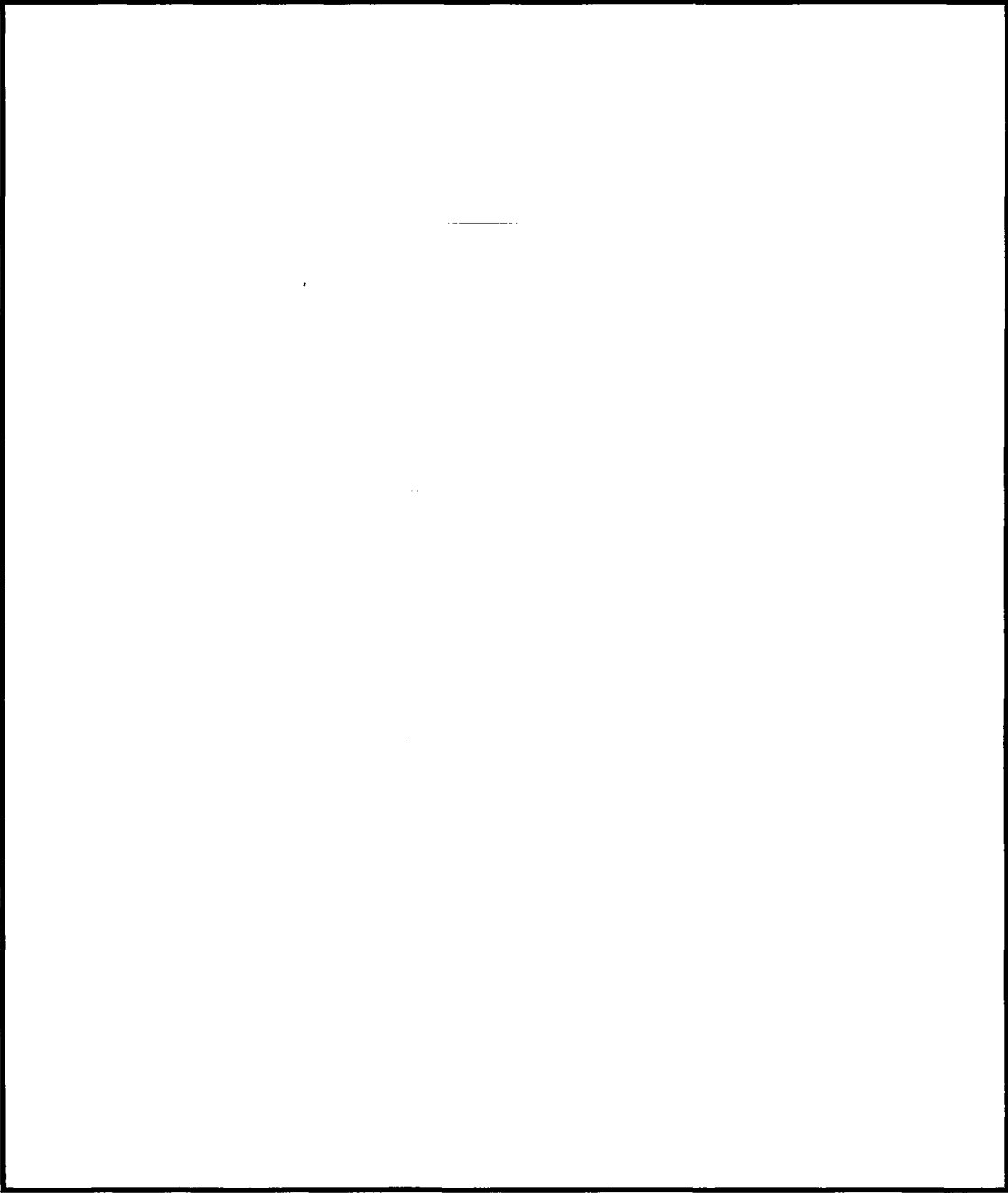
The DCS3000 to EDMS system is partly comprised of two (2) Dell 2850 Servers which both run Microsoft Windows 2000 Server. These servers have been secured according to NIST Standards. In the event that these servers need to be rebuilt, the installation disk(s) can be obtained by contacting the ISSO. The security configuration of the two servers has been captured via *INF* file and can also be obtained by contacting the ISSO.

2.1.1 Installation and Configuration Low Side

The DCS3000 to EDMS system is partially comprised of a CI-100 unit which is controlled by in-house software. In the event this software needs to be reconfigured the following are the steps that are necessary in order to insure the system is operational and stable:



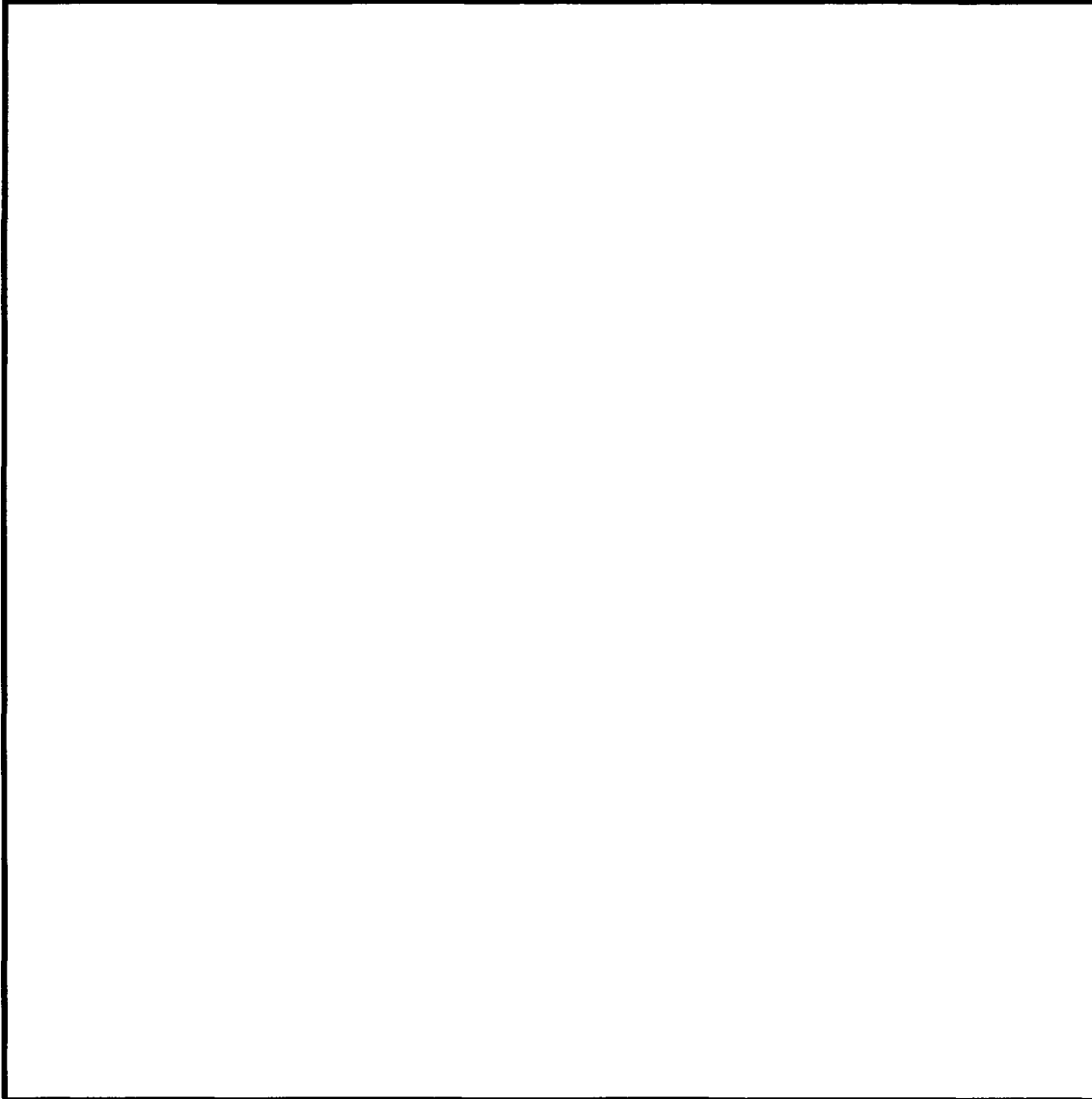
b2
b7E



b2
b7E

2.1.2 Configuring TCP UDP Software (*Low Side*)

The TCP UDP Software has a user friendly interface that allows the user to plug in the necessary criteria. The following attributes should be prescribed to the applicable field(s):



b2
b7E

TCP to UDP Converter

Protocol Connection

Route TCP Connections From:

Listen Port One

Enable Binding Address

Binding Address

Route UDP Connection To:

Send Address

Send Port

TcpUdp Router Name

OK

Cancel

TCP Keep Alive Disabled

b2
b7E

2.1.3 Configuring TCP UDP Software (*High Side*)

Configuring the High Side will be similar to configuring the Low side. The following should be prescribed to the applicable field(s):



b2
b7E

UDP to TCP Configuration

Protocol Connection

Route UDP Connections From:

Receive Port

Enable Binding Address

Binding Address

Route TCP Connection To:

Listen Port

Enable Binding Address

Binding Address

TCP Keep Alive
Disabled

TcpUdp Router Name

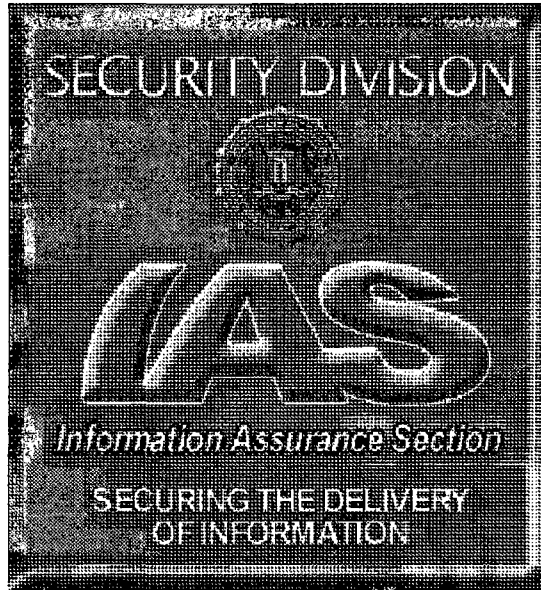
OK

Cancel

b2
b7E

~~SECRET~~

LIMITED OFFICIAL USE



**Controlled Interface – 100 (CI-100)
System Security Plan (SSP)
DCS-3000 to EDMS**

April 16, 2007

Version 1.0

Prepared For:



Unit Chief, Information Technology Security Unit
Federal Bureau of Investigation (FBI)
935 Pennsylvania Avenue, NW
Room 9483
Washington, DC 20530

b6
b7C

DATE: 06-05-2007
CLASSIFIED BY 65179DMH/KSR/LMF
REASON: 1.4 (G)
DECLASSIFY ON: 06-05-2032

Prepared By:
ITSU

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

LIMITED OFFICIAL USE
~~SECRET~~



LIMITED OFFICIAL USE

INTRODUCTION	7
1 INFORMATION SYSTEM GENERAL INFORMATION	8
1.1 Security Administration	8
1.1.1 System Information	8
1.1.2 Key System Points of Contact	8
1.1.3 Security Organization	10
1.1.4 Joint-Use Information	10
1.2 Mission	10
1.2.1 Purpose and Scope	10
1.2.2 Supported Projects	10
1.2.3 Information System Usage	10
2 SECURE FACILITY DESCRIPTION	11
2.1 Facility Layout	11
2.2 System Layout	11
2.3 Physical Environment	11
2.4 TEMPEST	12
3 SYSTEM DESCRIPTION	13
3.1 Summary	13
3.2 System Diagram	13
3.3 Personnel Security	14
3.4 Non-U.S. Citizens	14
3.5 Data Processed	14
3.5.1 Classification and Compartments	14
3.5.2 Dissemination Controls	14
3.6 Security Goals	15
3.6.1 Confidentiality	15
3.6.2 Integrity	15
3.6.3 Availability	15
3.7 Tier Level	15
3.8 Non-U.S. Citizen Users	15
3.9 Interconnection Interface Description	15
3.9.1 Direct Network Connections	15
3.9.2 Connectivity Management Procedures	15
3.9.3 Interconnection	15

3.9.4	Connectivity Procedures	16
3.9.5	Controlled Interface Requirements	16
3.9.6	Data Flow Diagram	17
3.9.7	Telecommunications Security	17
3.9.8	Networking	17
3.9.9	Indirect Connections	17
4	HARDWARE	18
4.1	Hardware Listing	18
4.2	Custom-Built Hardware	18
4.3	Configuration Management	20
5	SOFTWARE	20
5.1	Software Listing	20
5.2	Configuration Guides	21
5.3	Allowed Services and Protocols	21
5.4	Mail System	21
5.5	Foreign Software	21
5.6	Software with Restricted Access or Limited Use Requirements	21
5.7	Configuration Management	21
6	DATA STORAGE	22
6.1	Media Types	22
6.2	Media Handling	22
6.3	Backup and Restoration Process	22
6.4	Backup Protection	23
6.5	Disaster Recovery	23
7	SECURITY REQUIREMENTS	25
7.1	Threats & Vulnerabilities	25
7.2	User Access and Operation	25
7.2.1	Access Controls	25
7.2.2	Account Procedures	25
7.2.3	Authenticator(s) Procedures	26
7.2.4	System Users	26
7.2.5	Privileged Users	26
7.2.6	Password Changes	26
7.2.7	Password Generation	26

7.2.8	Log-on Error Handling	27
7.2.9	Account Lockout Handling	27
7.3	User Groups and Access Rights	27
7.3.1	User Groups	27
7.3.2	Non-data File Access	27
7.3.3	System Access Rights	27
7.3.4	Audit Logs	27
7.3.5	Privileged Users	27
7.3.6	Privileged Users Guides	28
7.3.7	Technical Access Mechanisms	28
7.3.8	Discretionary Access Control	28
7.3.9	Need-to-Know Controls	28
7.3.10	Mandatory Access Control	28
7.3.11	Discretionary Access Control Augmentation	28
7.4	Security Support Structure Protection	28
7.4.1	General	28
7.4.2	Trusted Communications	28
7.4.3	Validation Procedures	29
7.5	Security Features and Assurances	29
7.5.1	Incident Reporting	29
7.5.2	Remote Access	30
7.5.3	Configuration Management Program	30
7.5.4	System Assurance	31
7.5.5	Unique Security Features	31
7.5.6	Recovery Procedures	31
7.5.7	After Hours Processing	31
7.5.8	System Start-Up	31
7.5.9	Compliance-Monitoring Program	31
7.5.10	Non-Repudiation	32
7.5.11	Transaction Rollback	32
7.6	Auditing	32
7.6.1	Auditing Procedures	32
7.6.2	Notification Banner	33
7.6.3	User Accountability	33
7.6.4	Audit Protection	33
7.6.5	Audited Information	33
7.6.6	Audited Activities	33
7.6.7	Audit Review	34
7.6.8	Discrepancy Handling	34
7.6.9	System Verification and Testing	34
7.7	Marking and Labeling	35
7.7.1	System Hardware	35
7.7.2	Storage Media	35
7.7.3	Printout/Hardcopy	35
7.7.4	Internal Labeling	36
7.7.5	Exceptions	36
7.8	Maintenance Procedures	36
7.8.1	General	36
7.8.2	Uncleared Personnel	36
7.8.3	Logs	36
7.8.4	Maintenance Software	37
7.8.5	Remote Diagnostics	37

7.9	Sanitization and Destruction	37
7.9.1	Hardware	37
7.9.2	Data Storage Media	37
7.10	Software Security Procedures	37
7.10.1	Procurement	37
7.10.2	Evaluation	37
7.10.3	Malicious Code / Virus Protection	37
7.10.4	Data and Software Integrity Procedures	38
7.11	Media Movement	38
7.11.1	Media Introduction and Removal Procedures	38
7.11.2	Data Copying, Reviewing, and Releasing Procedures	38
7.12	Hardware Control	38
7.12.1	Transfer	38
7.12.2	Relocation	39
7.12.3	Release	39
7.12.4	Maintenance	39
7.12.5	Introduction	40
7.13	Web Protocol and Distributed/Collaborative Computing	40
7.13.1	Web Server / Clients	40
7.13.2	Mobile / Executable Code	40
7.13.3	Collaborative Processes	40
7.13.4	Distributed Processes	40
7.14	Wireless Devices	40
7.15	PKI Use	40
8	SECURITY AWARENESS PROGRAM	40
8.1	Program Description	40
8.2	Users' Guides	40
9	INTERCONNECTION SECURITY AGREEMENT	41
10	MEMORANDA OF AGREEMENT	41
11	AVAILABILITY	41
11.1	Restoration Procedures	41
11.2	Communications Back-up	41
11.3	Power Back-up	41
11.4	Denial of Service Prevention	41
11.5	Priority Process Protection	41
12	EXCEPTIONS	42

13	GLOSSARY OF TERMS	43
	APPENDIX A - ORGANIZATIONAL STRUCTURE	45
	APPENDIX B - FACILITY LAYOUT AND OVERVIEW	46
	APPENDIX C - SYSTEM EQUIPMENT LOCATION FLOOR PLAN	47
	APPENDIX D - SYSTEM HANDBOOKS	48
	APPENDIX E - RISK MANAGEMENT MATRIX	54
	APPENDIX F - CERTIFICATION TEST PLAN AND RESULTS	55

System Security Plan

INTRODUCTION

This system security plan (SSP) is for the *type* accreditation of the Controlled Interface-100 or CI-100. The CI-100 performs security domain adjudication of data transfer from an unclassified domain to a confidential/secret domain. This transfer is conducted via a modified networking medium, either a fiber optic cable or an RS-232 serial cable. This system is being accredited at the Tier-Two approval level with a high Confidentiality Goal, a high Integrity Goal, and a high Availability Goal. The CI-100 Security Concept of Operations (CONOPS) has been combined with this SSP.

1 INFORMATION SYSTEM GENERAL INFORMATION

1.1 Security Administration

This SSP supports the initial accreditation of the CI-100 system and due to the utility of the CI-100 configuration and its implementation at various operating locations, a *type* accreditation is warranted. This SSP is valid for three years or until a change to the architecture or configuration impacts the system security. In the event of a security incident involving the CI-100, the accreditation of the specific system should be reviewed.

1.1.1 System Information

This original SSP is for the type accreditation of the CI-100, a specially designed device used to transfer data from an unclassified network to a confidential/secret network. The CI-100 will always be treated as a single unit and will be limited to performing a single function - the transfer of data between the unclassified and confidential/secret security domains. A CI-100 is not permitted to connect a Tier 4 system to any other system.

1.1.2 Key System Points of Contact

The security administration for the CI-100 will vary by location. When a CI-100 is installed at a location, the local information systems security officer (ISSO) will identify and maintain a list of the following personnel: ISSO, information systems security manager (ISSM), system administrator(s), and the data owners of the connected systems. The following tables identify the points of contact for the CI-100:

Program Manager/System Owner

Name	[REDACTED]
Organization	Information Assurance Section (IAS), Security Division (SECD)
Telephone Number	202-324-[REDACTED]
Location	Room 7986, FBIHQ

Designated Accrediting Authority (DAA)

Name	William L. Hooton
Organization	Office of the Chief Information Officer
Telephone Number	202-324-[REDACTED]
Location	Room 11703, FBIHQ

Certification Official

Name	[REDACTED]
Organization	SECD
Telephone Number	202-324-[REDACTED]
Location	Room 7128, FBIHQ

Security Certification Official

Name	[REDACTED]
Organization	IAS, SECD
Telephone Number	202-324-[REDACTED]
Location	Room 1B948, FBIHQ

b6
b7C

DAA Representative

Name	
Organization	IAS, SECD
Telephone Number	202-324-
Location	Room, FBIHQ

Information Systems Security Officer (ISSO)

Name	[REDACTED]
Organization	OTD/ESTS/ETMU
Telephone Number	[REDACTED]
Location	ERF Quantico, VA

Information Systems Security Manager (ISSM)

Name	[REDACTED]
Organization	SecD
Telephone Number	[REDACTED]
Location	ERF Quantico, VA

b6
b7C

System Administrator #1

Name	[REDACTED]
Organization	OTD/ESTS/ETMU
Telephone Number	[REDACTED]
Location	ERF Quantico, VA

System Administrator #2

Name	[REDACTED]
Organization	OTD/ESTS/ETMU
Telephone Number	[REDACTED]
Location	ERF Quantico, VA

System Administrator #3

Name	
Organization	
Telephone Number	
Location	

Data Owner of Unclassified System

Name	[REDACTED]
Organization	OTD/ESTS/TICTU
Telephone Number	[REDACTED]
Location	ERF Quantico, VA

b6
b7C

Data Owner of Secret System

Name	[REDACTED]
Organization	OTD/ESTS/ETMU
Telephone Number	[REDACTED]
Location	ERF Quantico, VA



1.1.3 Security Organization

The information assurance architecture is currently under development by the Information Assurance Section, with ISSOs and ISSMs still being recruited. Once these personnel have been identified, the local ISSO will attach a list of security-pertinent personnel at their location and maintain the list with this packet. A basic organizational chart is found in Appendix A.

1.1.4 Joint-Use Information

Not applicable.

1.2 Mission

1.2.1 Purpose and Scope

The CI-100 acts as a controlled interface security device connecting an unclassified system (Low side) with a confidential or secret system (i.e., High side). The connection between the two security domains is accomplished by a "one-way transfer" (OWT) through the use of a modified RS-232 serial cable or fiber optic cable. The modified cable permits information to travel from the low side to the high side and eliminates the possibility of the high system from passing data to the low. This is accomplished by converting the data packets from TCP/IP to serial or UDP, both connectionless protocols. The data is pushed from the low side and across the OWT cable to the high system. Once on the classified system, the information is converted back to TCP/IP and sent out to the classified network.

USE OF THIS SYSTEM IS RESTRICTED TO DATA TRANSFERS FROM AN UNCLASSIFIED SYSTEM TO A CONFIDENTIAL/SECRET SYSTEM. UNDER NO CIRCUMSTANCES WILL AN UNCLASSIFIED SYSTEM BE CONNECTED TO A TOP SECRET OR A SENSITIVE COMPARTMENTED INFORMATION (SCI) SYSTEM OR THE DATA TRANSFER BE REVERSED, SENDING DATA FROM THE CLASSIFIED SYSTEM TO AN UNCLASSIFIED SYSTEM.

1.2.2 Supported Projects

The CI-100 can support any approved project where data needs to be moved from an unclassified system to a confidential/secret system.

1.2.3 Information System Usage

The only authorized use of this system is to provide a one-way transfer of data from an unclassified system to a confidential/secret system. Under no circumstances will it be used otherwise. Also, it will never be used to transfer data from a confidential/secret system to an unclassified system.

2 SECURE FACILITY DESCRIPTION

2.1 Facility Layout

As this is a *type* accreditation, a CI-100 can be deployed to a variety of different locations. However, there are some basic security requirements for the facility hosting the interface:

- The facility must be FBI-controlled space.
- The facility must be authorized for open storage of secret material on a hard disk drive.
- Access to the CI-100 must be restricted to only essential personnel (i.e., system administrators and ISSOs). General users should not be able to physically or logically access the system.
- Any uncleared visitors must be escorted when in the vicinity of the system.

The ISSO will provide a facility diagram and maintain it in Appendix B of this packet.

2.2 System Layout

The ISSO will provide a system layout diagram showing the physical location of the CI-100 and the systems to which it connects (if in the same location). This diagram will be maintained in Appendix C of this packet.

2.3 Physical Environment

The ISSO will annotate the approval date and authority for processing of classified information in this facility. If this approval does not state that open storage of secret information on the hard disk drive is permitted, then the approval date and authority for open storage will also be noted.

Facility Name	Location	Approval Date	Approval Authority	Classification Level	Open Storage?	Comments
ERF	Quantico, VA	2 November 1998	<div style="border: 1px solid black; width: 100px; height: 15px; background-color: black; margin-bottom: 5px;"></div> FBI\SecD\Security Operations\ Physical Security Unit	Secret	Yes	EC Case Number ID# 261D-HQ-C1062048-707

b6
b7c

A one-meter (39 inches) separation will be maintained between the unclassified and classified computers of this system. This separation also applies to other systems in the vicinity of the CI-100.

If a keyboard-video-mouse (KVM) switch is used, only an authorized KVM switch is permitted. The Information Assurance Section (IAS) of the Security Division can provide a list of authorized KVM switches.

All devices and media in the CI-100 will be properly marked with the appropriate classification labels. See subsection 7.7 for more information.

In most cases, the two computers that make up the CI-100 will be located in close proximity to one another (given the one-meter separation requirement). If the two systems must be located in two different locations, the fiber that connects the two computers will be encrypted or contained in a protected distribution system (PDS) if it passes through an area not authorized for handling classified data.

2.4 TEMPEST

Not applicable.

3 SYSTEM DESCRIPTION

3.1 Summary

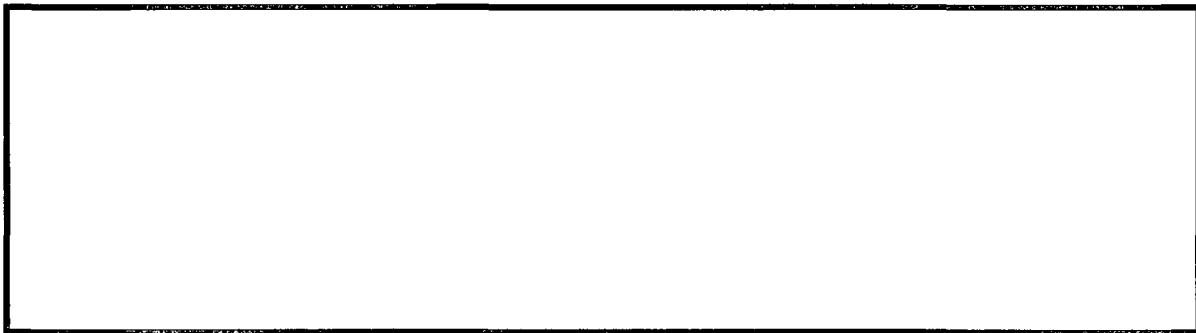
The CI-100 provides the technical ability to securely transfer digitized data from an unclassified system to a confidential or secret system. The movement of this data is technologically secure by using connectionless data protocols to push information across a modified networking medium. Each CI-100 is composed of two computers, one on the low (unclassified) side and one on the high (confidential/secret) side. Currently, this is accomplished by modifying a fiber optic or RS-232 cable so that it can only transmit data in one direction, from the low system to the high system.

A CI-100 computer can use a variety of operating systems although, currently, only Windows 2000 Professional or Windows 2000 server is authorized. The Windows operating system is hardened according to SANS (SysAdmin, Audit, Network, Security) Institute, National Institute for Science and Technology (NIST), and Common Criteria guidelines. All unnecessary services are turned off and unneeded ports blocked to limit the computer's exposure.

{S}

b1

Please see subsection 4.2 for a description of the customized hardware (i.e., NICs, fiber optic and RS-232 cables).



b2
b7E

Due to its unique capabilities and simplicity, the CI-100 can be deployed in a variety of environments. The goals for *integrity* and *availability* can vary from basic to high. As this is a type accreditation, it takes the most restrictive approach and is assigned a high goal for both integrity and availability. The *confidentiality* goal is also high, as information residing on the classified side of the network must be protected from disclosure.

Since all users (privileged users only) on this system have the appropriate security clearance, the need-to-know for all of the information on the system, and formal access approval, the CI-100 is a Tier Two (2) approval level system since it connects to other networks.

3.2 System Diagram

The CI-100 acts as an interface between two different networks, one unclassified, and the other, confidential or secret. The interface is composed of two computers, the low-side computer and the high-side computer. The low-side computer is unclassified and directly connects through a NIC (either fiber optic or RJ-45 based) to the unclassified network. The high-side computer is confidential or secret and directly connects through a NIC (either fiber optic or RJ-45 based) to the classified network. These two computers (the low and high-side computers) are connected using a modified fiber optic or serial cable that only permits data to be transmitted from the low to high computers. (If using a fiber optic cable, the NIC is also modified to enable this one-way

transfer.) Due to the cable's modifications, it is not possible for data to flow from the high-side system to the low-side.

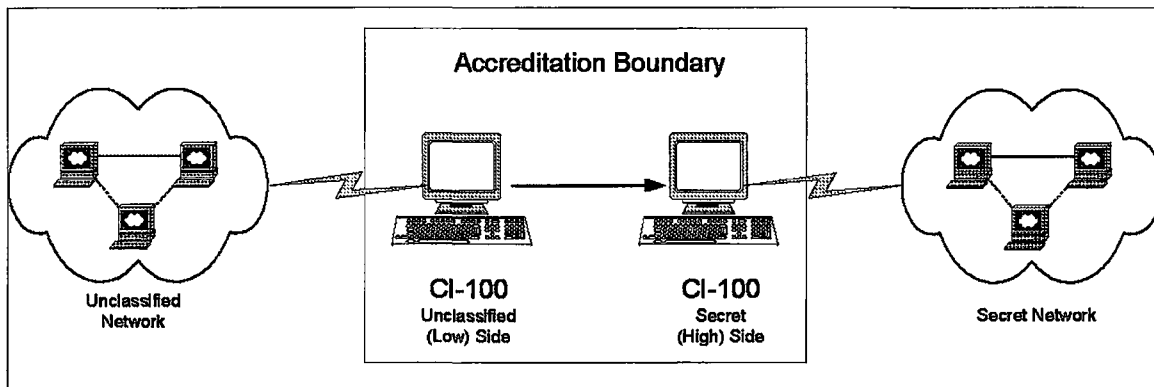


Figure 3-1 - Basic CI-100 Logical Diagram

3.3 Personnel Security

Any person authorized to access the system must have a minimum of a Secret clearance. These employees have an FBI Full Field Background Investigation (FFBI) or Department of Defense/Intelligence Community Single Scope Background Investigation (SSBI). The HQ or field office where the CI-100 is located will designate the system administrators authorized to maintain the system. The ISSO, system owner, and local security officer will verify that these administrators have the appropriate security clearance, formal access approval, and need-to-know for all of the information flowing through the interface prior to them being granted access to the system.

3.4 Non-U.S. Citizens

Non-US citizens are not authorized to use this system and are not allowed to maintain the CI-100. Foreign nationals may be authorized users on the two networks connected by the controlled interface but under no circumstances will they be allowed to physically or logically access the CI-100. The system administrator and ISSO will ensure that the device is protected from foreign users. This may entail the use of a tightly-controlled firewall or router-based access control lists (ACL) to prevent unauthorized access to the CI-100.

3.5 Data Processed

3.5.1 Classification and Compartments

Both classified and unclassified information is processed on a CI-100. When the information is on the low (unclassified) system, it is unclassified (i.e., information from the Internet) or sensitive-but-unclassified (SBU – i.e., law enforcement data). The information usually retains this classification after it is transferred to the high (Confidential/Secret) system. However, this information may be reclassified as confidential or secret when it is associated with information already residing on the high-side network.

3.5.2 Dissemination Controls

Information handled by the CI-100 may have the following handling caveats: Limited Official Use (LOU), For Official Use Only (FOUO), or Law Enforcement Sensitive (LES). The information usually retains this classification after it is transferred to the high

(Confidential/Secret) system. However, this information may be reclassified as confidential or secret when it is associated with information already residing on the high-side network.

3.6 Security Goals

3.6.1 Confidentiality

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

3.6.2 Integrity

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

3.6.3 Availability

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

3.7 Tier Level

<input type="checkbox"/> One	<input checked="" type="checkbox"/> Two	<input type="checkbox"/> Three	<input type="checkbox"/> Four
------------------------------	---	--------------------------------	-------------------------------

3.8 Non-U.S. Citizen Users

Not applicable.

3.9 Interconnection Interface Description

3.9.1 Direct Network Connections

The purpose of the CI-100 is to provide a logical connection between two different security domains, permitting unclassified data to flow into the classified system but not allowing classified information to leak to the unclassified system.

System Name	Classifications/ Compartments	Accreditation Date	Designated Accreditation Authority
EDMS	SECRET	18 August 2004	<input type="checkbox"/> SecD/AU
DCS-3000	SBU	28 May 2003	<input type="checkbox"/>

b6
b7C

3.9.2 Connectivity Management Procedures

Due its unique configuration, modifications to the CI-100 architecture are strictly controlled. The system is visually inspected weekly to verify that it has not been modified in ways that could adversely affect system security.

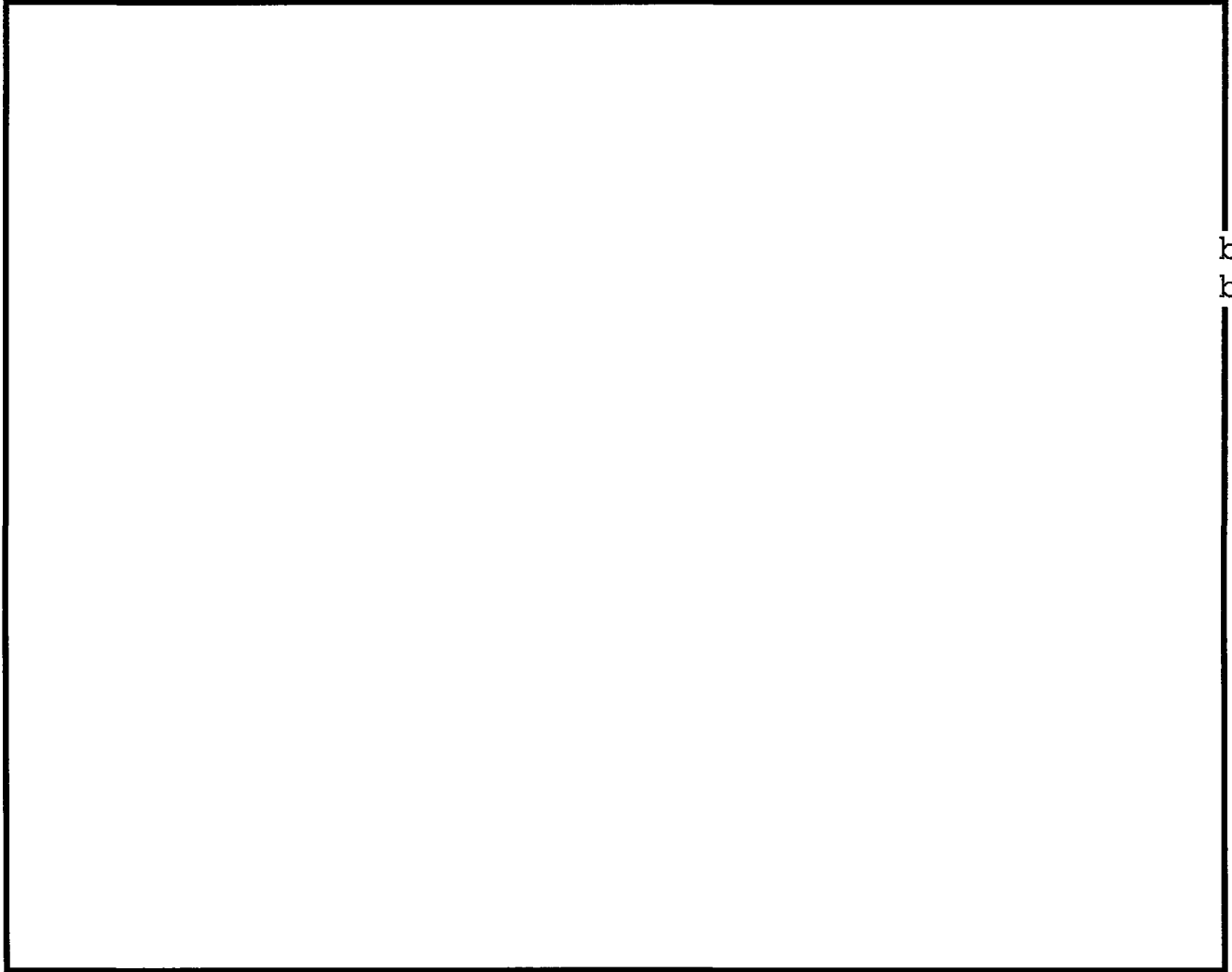
Physical access to the CI-100 will be restricted to system administrators, the only persons authorized to make any changes to the system. Prior to any additional connections being made, they will be reviewed by the system owner, program manager, and ISSM for possible system security impacts.

3.9.3 Interconnection

The system directly connected to the low-side of the controlled interface will conduct an anti-virus scan of all data prior to it entering the CI-100. This requirement is in addition to any other virus scanning conducted on the unclassified network. Once the data is on the high-side of the

CI-100, it is passed to the first node on the classified system. As it enters this network, the system directly connected to the high-side computer will scan all data arriving from the CI-100 before it is transmitted further into the classified network. This requirement is in addition to any other virus scanning conducted on the classified network.

3.9.4 Connectivity Procedures



b2
b7E

The CI-100 physical and logical configurations will not be changed without the approval of the DAA and program office. The ISO/ISSM must approve any repairs to the NIC and one-way cable. System administrators may conduct routine maintenance under their own authority.

3.9.5 Controlled Interface Requirements

The CI-100 will adjudicate the security policies between unclassified and confidential/secret security domains. The interface permits the electronic transfer of data from the unclassified system to the classified portion while preventing the leakage of classified information to the low side.

Since the CI-100 is a data transport mechanism, no data will be accessed on this system with the exception of reviewing packets causing networking problems. The packets will only be accessed to assess and resolve the problem. Only system administrators are permitted to perform these activities.

3.9.6 Data Flow Diagram

Data flows from an unclassified source, usually a network, through the controlled interface, and into a classified system. Due to the modified fiber optic/RS-232 cable, data cannot flow from the classified network to the unclassified network.

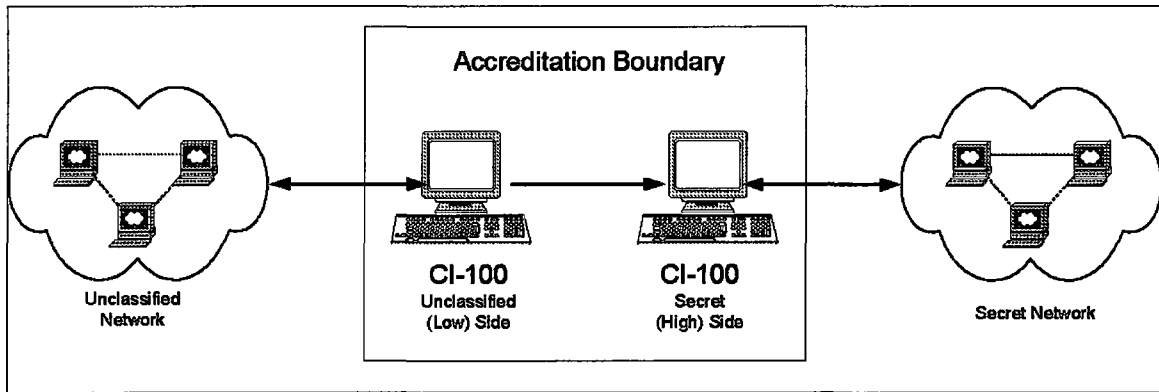
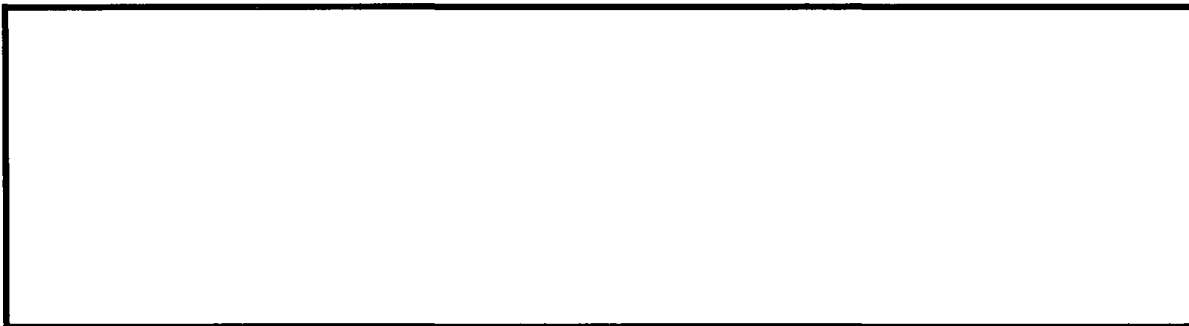


Figure 3-2 - Basic CI-100 Information Flow Diagram

3.9.7 Telecommunications Security

In most cases, the two computers that make up the CI-100 will be located in close proximity to one another (given the one-meter separation requirement). If the two systems must be located in two different locations, the fiber that connects the two computers will be encrypted or contained in a protected distribution system (PDS) if it passes through an area not authorized to process classified data.



b2
b7E

3.9.8 Networking

A CI-100 is a very basic computer network, two computers connected by a fiber optic or serial cable that can only transmit data from an unclassified machine to a classified one. There is no return transmission from the classified to unclassified system. Both systems are also connected to another network. The outside networks are usually based on TCP/IP and can use nearly any type of NIC (fiber optic, RJ-45 (Ethernet), etc.) to deliver data to/receive data from the CI-100.

3.9.9 Indirect Connections

The only indirect connections (sneaker-net) on the CI-100 are to provide software patches for the operating system or new code that facilitates the conversion of data between TCP/IP and UDP/serial. During normal day-to-day operations, the floppy and CDROM disk drives are

deactivated in the password-protected Basic Input/Output System (BIOS). The system administrator will activate the drives only when updated software or patches need to be applied.

4 HARDWARE

4.1 Hardware Listing

As this is a type accreditation, the specific information pertaining to the hardware being used will be different for each implementation. The ISSO will document the manufacturer, model, serial number, amount of RAM, hard disk size, and CPU speed. The ISSO will also identify the type of medium (i.e., fiber optic or RS-232) being used and name/source of the modified cable.

Computers

Manufacturer	Model	Serial Number	CPU Speed	RAM (MB)	Hard Disk Size	Classification
[REDACTED]						Unclassified
						Secret/
						Confidential

b2
b7E

One-way Transfer Medium

Cable Type	Source (POC)	Unit	Telephone Number
Fiber	[REDACTED]	OTD/ESTS/TICTU	[REDACTED]

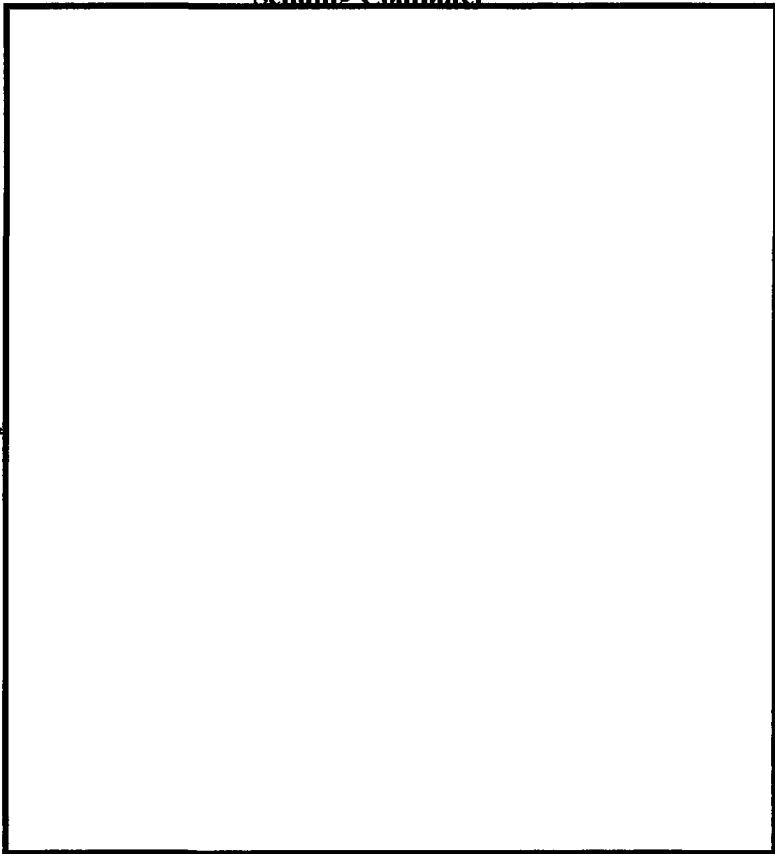
b6
b7C

4.2 Custom-Built Hardware

There are several pieces of customized hardware in the CI-100, modified fiber optic NICs and either a modified fiber optic cable or a modified RS-232 cable.

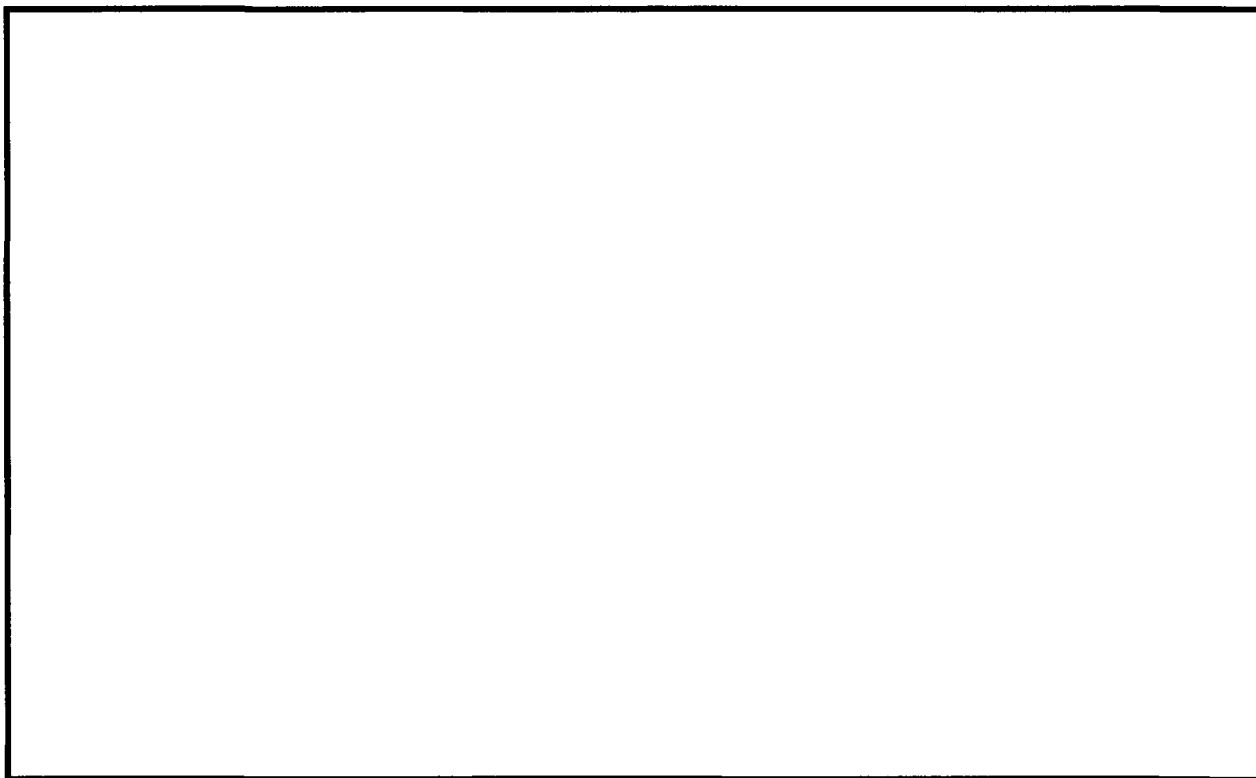
b2
b7E

Sending Computer



b2
b7E

Figure 4-1 - Fiber Optic-Based CI-100 Network Interface Card Connections.



b2
b7E

b2
b7E

Prior to the CI-100 being placed into operation between the two networks, it will be tested to verify that the low side can only transmit to the high side but cannot receive anything from that computer. The high side should be able to receive from the low side but not transmit to it. See subsection 7.5.9 for the basic testing procedures. The CI-100 must pass these tests before it can be installed.

4.3 Configuration Management

Configuration management (CM) is described in detail in subsection 7.5.3.

5 SOFTWARE

5.1 Software Listing

Very little software will be installed on the CI-100 since the system performs critical security functions. To help limit the number of system vulnerabilities that non-essential programs may introduce, these unneeded programs are not found on the system.

The only operating system authorized for use in the CI-100 is Microsoft Windows 2000 Professional with Service Pack 3a or Windows 2000 server with Service Pack 4. The operating system will be hardened prior to being placed into operation. These hardening procedures are based on information security best practices and guidance documents from NIST, the SANS Institute, and Common Criteria. The hardening procedures and/or scripts are found in Appendix D.

(S)

b1

Up-to-date antivirus software will be used on the CI-100 to prevent an infection passing from the low side to the high side. The program must be properly configured so that in the event malicious software is detected, it isolates the offending program in the computer and permits the continued flow of data through the CI-100. For further information, please see subsection 7.10.3.

b2
b7E

The following is a list of software found on the CI-100:

- The TCP/IP – UDP/Serial conversion and reversion programs
- Microsoft Windows 2000 Server with Service Pack 4
- Adobe Reader 6.0.1
- WinZip 10.0
- McAfee Virus Scan Enterprise Version 7.0.0.511

5.2 Configuration Guides

The operating system configuration guides are found in Appendix D.

5.3 Allowed Services and Protocols

a. Services internal to the CI-100:

telnet

b. Services outside the boundary of the LAN:

SSL

SSH

telnet

c. Network Protocols:

UDP

TCP/IP

RS-232/Serial
connectivity

FTP

ICMP

5.4 Mail System

Not applicable.

5.5 Foreign Software

There is no foreign software on the CI-100. However, due to the way the software industry is currently developing programs, non-U.S. citizens are likely to have worked on building the anti-virus software and the operating system.

5.6 Software with Restricted Access or Limited Use Requirements

The security of the entire CI-100 system is based on a severely restricted access list. As such, use of all software on the CI-100 is restricted to system administrators.

5.7 Configuration Management

Configuration management (CM) is described in detail in subsection 7.5.3.

6 DATA STORAGE

6.1 Media Types

Various types of data storage media are used on the CI-100, but hard drive storage is predominant. The hard drive contains the hardened operating system, the TCP/IP-to-UDP or RS-232 conversion program, and the anti-virus program. Data being transmitted over the controlled interface is not stored on either of the CI-100 machines. The last node on the unclassified network retains copy of the data until it is either manually or automatically deleted. When configuring this system, the system administrator must build in enough time to review the file transfer audit logs on the high-side system to identify any packets that did not arrive intact. If a packet was corrupted in transmission, the system administrator must manually resend the packet from the unclassified network and verify that the packet was received intact.

Floppy disks and CD-ROMs are used on a sporadic basis and only to load updates to software already on the system. On a day-to-day basis, the floppy and CD drives will be deactivated in the password-protected BIOS. When software updates or new software need to be loaded onto the system, the system administrator will reactivate the floppy and/or CD drives in order to perform these tasks. Once the software is loaded, the drives will be deactivated.

6.2 Media Handling

All media are handled in accordance with its classification. If the facility is not authorized for open storage of hard-copy Secret material, but open storage is permitted for non-removable magnetic media, all Secret removable media (floppy, CDs, Zip disks, etc.) will be secured in a GSA-approved safe. If the facility that houses the CI-100 is **not authorized** for the open storage of **any** classified information, the CI-100 will be built with removable hard drives. These drives would be secured in a GSA-approved safe at the close of business.

All removable media are marked with the appropriate SF 7xx classification and data descriptor labels. An unclassified disk will be marked with the green SF 710, Confidential with the blue SF 708, and Secret with the red SF 707. All removable media will also have a white SF 711 Data Descriptor label affixed to its surface. Fixed hard disk drives do not need to have the labels on their cases as the labels attached to the CPU cases are sufficient. Removable hard drives and hard drives removed from the CPU case will have classification and data descriptor labels.

In most cases, removable media are classified in accordance with the classification of the system in which they are used. This means that a disk containing only unclassified information but used on a secret system is classified secret. However, there is an exception to this rule. If the system administrator or ISSO write-protects an unclassified floppy disk, the disk may be used in a classified system and retain its "Unclassified" markings. Write-protecting the disk ensures that classified information is not inadvertently written to the floppy. The case is similar for CD-ROMs. If the classified machine's CD-ROM drive is a read-only drive and *not* a CD-RW (Read/Write) drive, the unclassified CD-ROM can be used in a classified machine and still retains its "Unclassified" status.

For clearing, purging, and destruction of media, please see paragraph 7.9.1.

6.3 Backup and Restoration Process

Very little data is maintained on a CI-100. Unless otherwise authorized by the DAA, the only programs authorized to be on the systems are the operating system and the data-conversion programs. No operational data (data to be transferred) is maintained on the CI-100. The system

administrators will keep a local floppy/CD-based version of the CI-100 configuration settings and the data conversion programs. This disk should not be stored in the vicinity of the CI-100. Additionally, the Information Assurance Section, Security Division, will maintain an e-mailable copy of the operating system settings and the data conversion programs that can be quickly sent to a site needing them.

6.4 Backup Protection

As stated in the previous paragraph, backup copies of the operating system configuration and the data conversion programs are maintained locally and at the FBIHQ. The operating system (Windows 2000 Server) is widely available, either commercially or from FBIHQ. The hardening procedures are unclassified with the associated public domain information built from several trusted sources. The conversion program is the only software that needs additional protection as it is government-off-the-shelf (GOTS) software and is labeled *Limited Official Use/For Official Use Only*.

Generally, there are no special security requirements for the CI-100 hardware and firmware since they are readily available. With the exception of the modified NICs, fiber optic cables, and serial cables, the CI-100 computers can be pulled from excess equipment within the FBI. The hardware specifications for the CI-100 computing platforms are not extensive and do not require top-of-the-line computers. The system administrator will identify sources of spare computers, NICs, and cables to assist in expediting the computer replacement.

6.5 Disaster Recovery

A CI-100 Disaster Recovery pack will be maintained, preferably offsite, but readily available. It will consist of:

- At least one copy (if not both copies) of the operating system CD-ROMs
- The operating system configuration file
- The TCP/IP to UDP or RS-232 conversion program
- At least two modified fiber optic or serial cables
- The system administrator manual
- A copy of the CI-100 SSP

Additionally, the system administrator will maintain a list of possible hardware sources to replace the CI-100 components in the event that the system must be rebuilt from scratch. Particular attention must be made to sources of the fiber optic NICs as they usually do not come as standard equipment on PCs.

In the event a CI-100 must be reconstructed from scratch, the system administrator will adhere to the following procedures.

- Identify a new location for the CI-100, paying particular attention to the ability to connect the two networks, authorized to process classified information, power, air conditioning, physical security, environmental hazards, etc.
- Set-up the new computers, mark them with the appropriate classifications, and load the base operating system as well as any authorized services packs and security patches.
- Once the operating system is loaded, harden the system using the automated scripts on the CI-100 program CD-ROM or by manual configuration.

- Configure the network settings on the high and low-side computers.
- Connect the OWT cable to the low-side computer matching the green end of the cable to the unclassified machine. Connect the blue/red end of the cable to the classified machine.
- Conduct basic networking tests to verify that the OWT cable is actually one-way. (See subsection 7.6.9.)
- If all of the basic networking tests fail, the CI-100 has been assembled properly.
- Install the data conversion programs on the low and high-side computers.
- The connections to the two outside networks may be established and the interface can resume transmitting data.

In the event of a power loss, the system administrator must ensure that the high side of the CI-100 is brought online before the low side. This will prevent data from being lost when the low side, which blindly transmits the UDP data packets, broadcasts packets to the high side that is incapable of receiving data as it is still off-line.

In a similar situation, if the system administrator must take the system off-line, the low side of the CI-100 must be taken down before the high side, thus preventing the low side from broadcasting packets to a system that is no longer functioning.

Each site will integrate its site-specific disaster recovery/continuity of operations plan into this SSP as well as into their parent division's plans.

7 SECURITY REQUIREMENTS

7.1 Threats & Vulnerabilities

Please see Appendix E, *Risk Management Matrix*.

7.2 User Access and Operation

7.2.1 Access Controls

All system users have unique identifiers that permit the tracking of each individual's actions on the system. Passwords are the chosen method of authentication. Additionally, FBI spaces have several layers of physical security controlling physical access to CI-100s and other systems.

b2
b7E

[REDACTED] To gain access to FBI facilities, two forms of identification are required, one of which is usually a proximity-type badge verifying that the person has a completed security background investigation.

Once inside FBI spaces, all personnel must display their security badge. The badge by itself or in conjunction with a PIN can grant employees access to various rooms. Access to rooms containing a CI-100 is controlled to only those personnel with the proper security clearance, an established need-to-know, and formal access approval for all information flowing across it.

Currently, only user IDs and passwords are used for identification and authentication. There are two user groups on the CI-100, the system administrator and ISSO groups; no general users are allowed on the system.

7.2.2 Account Procedures

During the hardening procedures for the system, all default accounts are renamed and any guest account is deactivated. The renamed default system administrator account is used to create the initial unique user ID system administrators accounts and grants system administrator privileges to these unique accounts. These accounts have full privileges to the system with the exception of full access to the system audit logs; the accounts only have read access to the logs.

The renamed default system administrator account will create the ISSO group and accounts. This group will have full access to the system audit log files, but only general privileges on the remainder of the system.

[REDACTED]

b2
b7E

[REDACTED] If a new system administrator account needs to be established, an existing system administrator will create the account and grant system administrator privileges to it.

The number of system administrator and ISSO accounts will be kept to an absolute minimum. Only employees with the proper security clearance, an established need-to-know, and formal access approval for all of the information flowing across it will be assigned an account.

Accounts on this system are not modified. In the event an account needs to be terminated, it is removed from the system. However, a record will be maintained of that user ID and the person who used it. This information will be retained for a period of 90 days as the audit logs for the

system must be maintained for that period of time. This user ID record will associate the user ID, the actual name of the system administrator/ISSO, and past actions he/she has taken on the controlled interface.

7.2.3 Authenticator(s) Procedures

[Redacted]

b2
b7E

Automated password strength checkers and generators are not used. System administrators and ISSOs are briefed on how to construct a strong password.

[Redacted]

b2
b7E

[Redacted] Often, only one system administrator is on duty at a given time [Redacted]

7.2.4 System Users

There are no general system users on the CI-100.

7.2.5 Privileged Users

All privileged users have unique user IDs and unique passwords. However, see subsection 7.2.3 concerning use of the renamed default system administrator account.

7.2.6 Password Changes

[Redacted]

b2
b7E

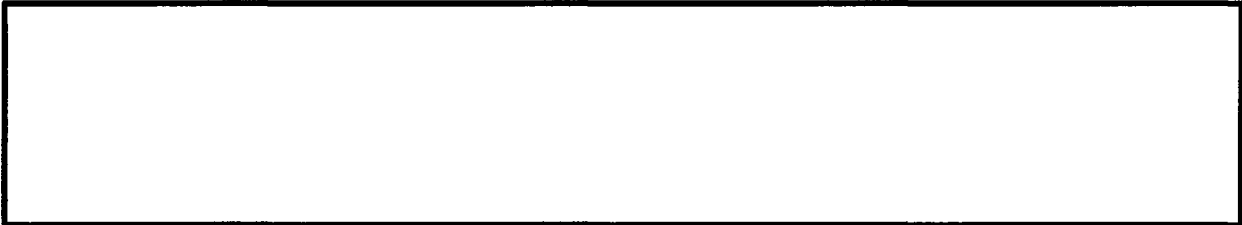
7.2.7 Password Generation

Automated password strength checkers and generators are not used; system administrators and ISSOs are briefed on how to construct a strong password.

7.2.8 Log-on Error Handling

A user is locked out of his/her account after a maximum of four attempts, and a system administrator must unlock the account.

7.2.9 Account Lockout Handling



b2
b7E

7.3 User Groups and Access Rights

7.3.1 User Groups

The two user groups on the CI-100 are the system administrator and ISSO groups. In order to become a system administrator, one must have the proper security clearance, an established need-to-know and formal access approval for all of the information flowing across the interface. To become an ISSO, one must also have the proper security clearance, an established need-to-know, and formal access approval for all of the information flowing across the interface. Additionally, the ISSO needs to be technically proficient on the operating system on the CI-100 and have security training or a security background.

7.3.2 Non-data File Access

System administrators can change the configuration and/or content of all files other than the system audit log files on the CI-100 since they have complete control of the system. However, only the ISSOs are allowed to have full privileges to the system audit log files.

7.3.3 System Access Rights

The system administrator group can set privileges for all users on the system. System administrators have complete control of their systems with the exception of having full privileges to system(s) audit log files.

7.3.4 Audit Logs

Users (system administrators) can view the audit log but cannot change or delete it. The ISSO can view and delete the audit log. The ISSO is the only person authorized to transfer the audit logs from on-line storage to off-line storage.

7.3.5 Privileged Users

There are three (3) privileged users on this system. There are two categories of privileged users - system administrators and the ISSO. The privileges granted to the ISSO are less than those of the system administrator with one exception - the ISSO has full control over the audit log. This is necessary, as the ISSO must transfer the audit logs from on-line storage to off-line storage. The system administrators can only view the audit log file. For a list of auditable events, please see subsection 7.6.

7.3.6 Privileged Users Guides

Please see paragraph 8.2.

7.3.7 Technical Access Mechanisms

Although the FBI policy states that the password-protected screen lock must activate after 20 minutes of user inactivity, the screen lock on the CI-100 will activate after five (5) minutes of inactivity. It is highly recommended that if the system administrator steps away from the CI-100 terminal, he/she immediately activates the password-protected screen saver by pressing Alt-Ctrl-Delete and selecting the Lock Workstation button.

7.3.8 Discretionary Access Control

System administrators have full control over all files on the CI-100 except for the audit log files. ISSOs have full control over audit logs, whereas system administrators can only view the logs.

7.3.9 Need-to-Know Controls

System administrators and ISSOs have established need-to-know for all of the information flowing through the CI-100.

7.3.10 Mandatory Access Control

Not applicable.

7.3.11 Discretionary Access Control Augmentation

Not applicable.

7.4 Security Support Structure Protection

7.4.1 General

The security support structure consists of three primary elements - the OWT medium, the systems logs (i.e., audit and data transfer logs), and the operating system configuration. The OWT medium ensures that unclassified data can be transferred to the classified side, but classified information cannot leak down to the unclassified devices. The audit logs enable the ISSO to identify general system activity by type of activity and user ID (Please see specific information in subsection 7.6.). The data transfer logs permit the system administrator to view the number of packets sent, received, and any that were modified during transmission. Finally, the operating system configuration is hardened according to tested configurations. The configuration will not be changed without following the FBI Configuration Management process and being approved by the ISSM and DAA.

7.4.2 Trusted Communications

Not applicable.

7.4.3 Validation Procedures

The certification test plan/results (CTP/R) from the certification testing of the Microsoft Windows 2000 Professional/Server-based CI-100 are found in Appendix F.

On at least a daily basis, the system administrator will review the data transfer logs to identify any packets that were modified in transit. If a significant amount of traffic is transmitted on a daily basis, this review should occur every 2-4 hours.

On a weekly basis, the ISSO will verify and document the following items:

- Verify that the OWT medium (fiber optic or RS-232 cable) has not been replaced and continues to be plugged in to the proper computer (green end to low system, red/blue to the high system)
- Verify that the warning labels on the OWT medium and the computer systems have not been removed
- Verify that the network interface cards (NIC) have not be replaced and the send port on the high system and the receive port on the low system are still epoxied shut
- Review the CI-100 audit logs for any anomalous activity

Every six months, the system administrator and ISSO will attempt to ping the high system from the low system. This test should time out as the (Internet Control Messaging Protocol (ICMP) packets are sent to the high side, but no replies should be received, as the high system should not be able to send reply packets to the low system. They will try to ping the low side from the high side, but the attempt should fail, as packets cannot be sent from the high to the low side. Following the ping attempts, the system administrator and ISSO will attempt to establish a telnet session between the low and high systems. Both attempts should fail since there is no way to establish the handshake necessary for the session. These test results will be documented.

All verification and validation result logs will be maintained with this SSP until the CI-100 is reaccredited.

7.5 Security Features and Assurances

7.5.1 Incident Reporting

The following types of incidents should be reported through the ISSO to the ISSM:

- Compromise of classified information as a result of an individual's misuse of the CI-100, or failure to follow rules, procedures, guidelines, or regulations pertaining to system use
- System failures that result in the compromise of classified information
- Hostile penetration attempts
- Flaws or vulnerabilities that could result in the compromise of classified information
- Unauthorized configuration changes to the operating system or hardware
- Malicious code response
- System contamination where data has leaked from the high side to the low side

For any incident where classified information has or is suspected to have been compromised, the following procedures will apply:

- Cease activity and disconnect the CI-100 from both networks. If this is a high-availability system, another CI-100 will be built using the steps outline in subsection 6.5, *Disaster Recovery*, and put into place. The ISSO and Security Officer will conduct a preliminary determination on the extent of the compromise or contamination.
- Immediately contact ISSM and Enterprise Security Operations Center (ESOC) to report the incident. Further guidance will be provided as dictated by the circumstances.
- Identify the originator or source of the incident and identify all receivers (e.g., systems, users) of the data.
- Prior to bringing the affected system back on line, coordinate specific actions to be taken to with the ISSM.
- A written report of the incident is to be provided to DAA within three (3) business days of completing clean-up.

The program manager will maintain a list of security incidents to identify patterns that may indicate potential CI-100 design problems.

7.5.2 Remote Access

Remote access to a CI-100 is not authorized. The DAA may grant exceptions for remote management of the system. If granted, all remote management activities will take place via an encrypted session. A copy of the exception will be maintained with this packet.

7.5.3 Configuration Management Program

The following paragraphs are based on *the FBI Configuration Management Policy for IT Projects*, Version 1.0 attached to an EC dated 10/01/2001 (Case ID # 66F-HQ-A1315416).

(S) The CI-100 is composed of two tightly-configured PCs that are connected by a modified cable so data is securely transferred from an unclassified system to a classified system. The computers operating systems are tightly configured using Common Criteria, NIST [redacted] and SANS guidance. Only the IAS can authorize changes to these settings or allow patches to be installed on the computers. IAS will maintain and update configuration settings for the CI-100 and is the only authorized source for these configuration files. IAS will also provide guidance and act as a trusted source for any operating system patches. The ISSM/ISSO will serve as the conduit for changes to the controlled interface and provide assistance to the system administrator in receiving approval for possible field-recommended system changes. The system administrator will maintain a configuration log, annotating all changes to the CI-100.

b1

All systems shipped will have a primary and spare modified cable to permit quick replacement of a failed medium. Instructions for making a new modified cable are provided in subsection 4.2.

In the event a NIC fails, subsection 4.2 provides guidance on how to replace and configure a fiber optic NIC in a CI-100.

Prior to any changes to the system architecture or operating system configuration, the program office (i.e., IAS) will make the changes on a non-operational system in a test environment. A full-scale system vulnerability test, similar to the ones conducted for this accreditation, will be performed on the test system and ensure that the proposed changes do not have a negative impact on system security. Only after the vulnerability testing is completed and risks are mitigated will

a new version of the CI-100 be fielded. (Please see subsection 7.6.9 for system verification and testing procedures.)

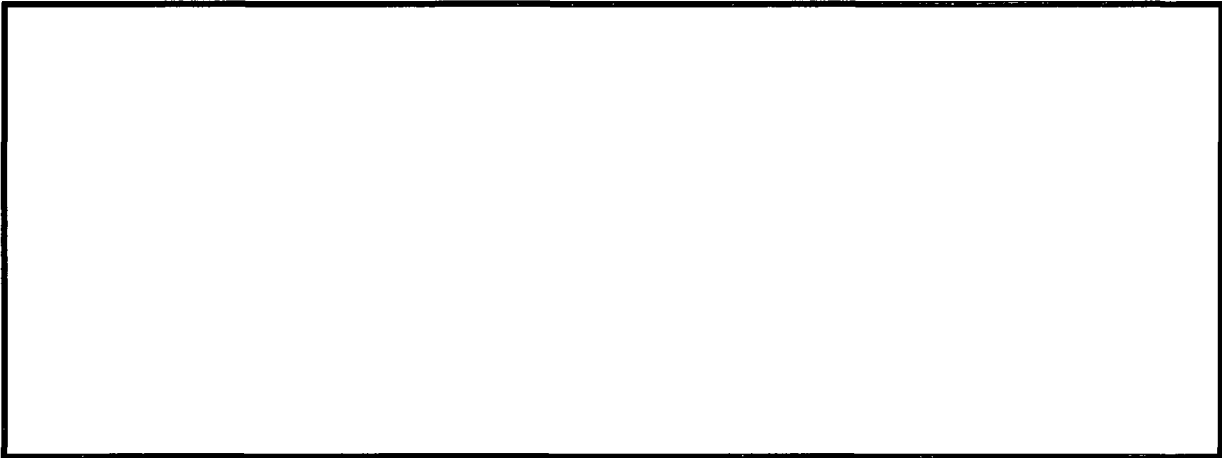
7.5.4 System Assurance

Please see subsections 7.4.3 and 7.6.9.

7.5.5 Unique Security Features

The unique security feature in the CI-100 is the one-way transfer of data from an unclassified system to a confidential/secret system. For a detailed description, please see subsections 3.1 and 4.2.

7.5.6 Recovery Procedures



b2
b7E

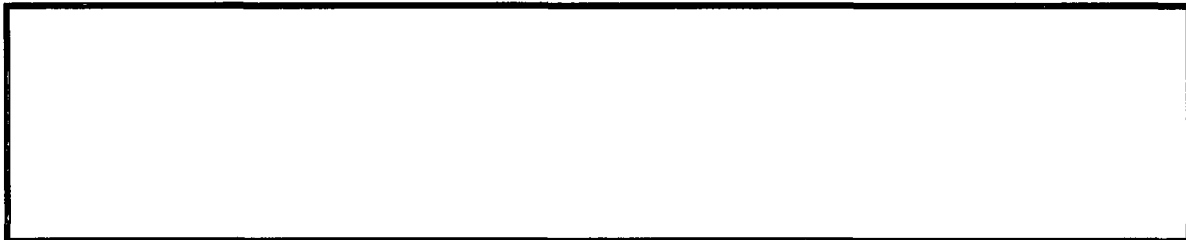
In the event of component damage, please refer to subsections 4.2 and 6.5 on the procedures to take when replacing systems and configuring them properly.

If the above steps are taken, the CI-100 will recover to a secure mode and ensure that information continues to flow across the one-way medium.

7.5.7 After-Hours Processing

Most CI-100s will be operational 24/7 to facilitate the flow of information between the two security domains.

7.5.8 System Start-Up



b2
b7E

7.5.9 Compliance-Monitoring Program

On a periodic basis, the ISSO and system administrator will verify various aspects of the CI-100 Security Support Structure and system configuration.

On a weekly basis, the ISSO will verify and document the following items:

- Verify that the OWT medium (fiber optic or RS-232 cable) has not been replaced and continues to be plugged into the proper computer (green end to low system, red/blue to the high system).
- Verify that the warning labels on the OWT medium and the computer systems have not been removed.
- Verify that the Network Interface Cards have not be replaced and the send port on the High system and the receive port on the Low system are still epoxied shut.
- Review the CI-100 audit logs for any anomalous activity.

Every six months, the system administrator and ISSO will attempt to ping the high system from the low system. This test should time out as the ICMP packets are sent to the high side, but no replies should be received since the high system should not be able to send packets to the low system. They will try to ping the low side from the high side, but the attempt should fail as packets cannot be sent from the high to the low side. Following the ping attempts, the system administrator and ISSO will attempt to establish a telnet session between the low and high systems. Both attempts should fail, as there is no way to establish the handshake necessary to establish the session. These results will be documented.

All verification and validation result logs will be maintained with this SSP until the CI-100 is removed or reaccredited.

7.5.10 Non-Repudiation

Non-repudiation is applied to all privileged user activities on the system. User IDs are used to identify these activities and the information is entered into the audit log.

7.5.11 Transaction Rollback

Transaction rollback is not conducted on this system. The only activities that could be rolled back are operating system patches. In the event a patch needs to be installed or removed, configuration management procedures are applied. These activities are logged into the audit log or maintained in the hard-copy configuration management log.

7.6 Auditing

7.6.1 Auditing Procedures

There are two types of auditing on the CI-100, auditing at the operating system level and at the file transfer level (on the high-side machine). The low and high-side machines monitor activities at the operating-system level for the system administrator and ISSO user groups. Additionally, on the high-side machine, all arriving files are logged as to the file name, date arrived, file size, and the MD5 check sum attached to the incoming file and a second checksum generated on the high-side system to verify that the file arrived unaltered.



7.6.2 Notification Banner

At log-on, the standard DOJ warning banner employed by the FBI appears, and the user must positively acknowledge agreement or access is denied.

The text of the warning banner is as follows:

WARNING! This computer system is the property of the United States Department of Justice. The Department may monitor any activity on the system and search and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored on the network and stored locally on the hard drive or other media in use with this unit (e.g., floppy drives, CD-ROMS, etc.).

7.6.3 User Accountability

Each user is issued a unique user ID and is held responsible for his/her actions. Account management procedures are found in subsections 7.2 and 7.3.

7.6.4 Audit Protection

The audit trail is protected from unauthorized modification. All users can view the audit log; however, only the ISSO is allowed to modify/move the audit log.

7.6.5 Audited Information

The following information is found within the audit trail:

- User ID
- Date of activity
- Time of activity
- Type of event or action
- Terminal ID from/on which action was taken
- Success/failure of the event

7.6.6 Audited Activities

The following items are audited (success and failure):

- Log-on/off
- Use of privileged user or root privileges
- Attempts to change data
- Deletion of files, directories, or data elements
- Access to security-relevant directories, objects, and incidents
- System console activities
- Change of formal access permissions
- Attempted access to objects or data whose labels are inconsistent with user privileges
- Attempts to modify the audit trail file

- Movement/deletion of the audit trail file

7.6.7 Audit Review

On a weekly basis, the ISSO will review the operating system audit trail. These files will be retained on-line for one month and off-line for five years.

On a minimum of a daily basis, the system administrator will review the file transfer audit trail to identify any files that may have been corrupted or altered during transmission. It is unnecessary to maintain an on-line copy of more than the last 24 hours activity. This audit trail will be maintained on-line for 90 days.

7.6.8 Discrepancy Handling

In the event there is a discrepancy or indications of possible suspicious activity, the ISSO will conduct an initial inquiry into the matter. If deemed suspicious, the ISSO will notify the ISSM, system owner, and the appropriate security officer of the activity. Then, the FBI incident-handling procedures will be followed. If benign, the discrepancies will be logged into a memorandum for the record and placed in the ISSO's files. In the event of multiple occurrences of the same discrepancy, the ISSO and system administrator will identify the source of the discrepancy and resolve the problem.

7.6.9 System Verification and Testing

On a daily basis, the system administrator will verify that the conversion and transfer mechanisms are functioning properly. This is done by reviewing the transfer log on the high-side system to identify any packets that have been corrupted during transmission. If an unusual number of packets have been corrupted, the system administrator will attempt to identify the problem. If unable to rectify the problem, the system administrator will notify the ISSO, ISSM, and program manager of the difficulties. Once a solution is devised, it will be disseminated to the organization having the problem.

On a periodic basis, the ISSO and system administrator will verify various aspects of the CI-100 Security Support Structure and system configuration.

On a weekly basis, the ISSO will verify and document the following items:

- Verify that the OWT medium (i.e., fiber optic or RS-232 cable) has not been replaced and continues to be plugged into the proper computer (green end to low system, red/blue to the high system)
- Verify that the warning labels on the OWT medium and the computer systems have not been removed
- Verify that the NICs have not been replaced and that the send port on the high system and the receive port on the Low system are still epoxied shut
- Review the CI-100 audit logs for any anomalous activity.

Every six months, the system administrator and ISSO will attempt to ping the high system from the low system. This test should time out as the ICMP packets are sent to the high-side, but no replies should be received, as the high system should not be able to send packets to the low system. They will try to ping the low side from the high-side, but the attempt should fail, as packets cannot be sent from the high to the low side. Following the ping attempts, the system administrator and ISSO will attempt to establish a telnet session between the low and high

systems. These attempts should also fail, as there is no way to establish the handshake necessary to establish the session. All results will be documented.

All verification and validation result logs will be maintained with this SSP until the CI-100 is removed or reaccredited.

Intrusion detection systems (IDS) are not used on the CI-100. If use of an IDS is required/desired, it should be placed on the networks to which the controlled interface connects. The certification test plan/results are found in Appendix F.

7.7 Marking and Labeling

7.7.1 System Hardware

All CI-100 computers are labeled in accordance with the classification of the information they process or the network to which the computers are connected. Low-side computers are labeled with green SF 710 stickers on the front of their CPUs. In many cases, rack-mounted computers are being used as the two computers that comprise the CI-100. In the event there is not room on the front of the chassis for a SF 710 label, green tape will be used to mark the entire front top edge of the device to signify its classification. A SF 710 will fold over the front top edge of the computer as much as possible. Additionally, the rear of the computer will be marked in a similar manner, either an SF 710 placed on the back of the device or the rear top lip will be edged by green tape.

The front of the high-side CPU will be have a red SF 707 (Secret) or blue SF 708 (Confidential) label affixed to it. As with the low-side rack-mounted computer, the front top and rear top lips of the high-side device will have colored tape (matching the color of the SF label) and an overlapping SF label affixed to them.

The OWT medium (i.e., fiber optic or RS-232 cable) will also be marked with colored tape. The transmitting end will have the last two to three inches of the cable covered by green tape. The receiving end of the cable will have the last two to three inches of the cable covered by red (Secret) or blue (Confidential) tape. This provides a quick means for the system administrator and ISSO by which to quickly verify that the correct ends of the cable are plugged into the proper computer. The green end of the cable is plugged into the green computer; the red/blue end of the cable is plugged into the red/blue computer.

Above the modified NICs, both computers will also have a label stating, **"DO NOT REPLACE ANY NIC WITHOUT THE PERMISSION OF THE ISSO."** A similar label will be placed on the OWT medium stating, **"DO NOT REPLACE THIS CABLE WITHOUT THE PERMISSION OF THE ISSO."**

7.7.2 Storage Media

Please see subsection 6.2.

7.7.3 Printout/Hardcopy

Hardcopy printouts will not be made on this system. Printers will not be connected to the CI-100.

7.7.4 Internal Labeling

Initially, all information crossing the CI-100 is unclassified. Once it has been transmitted from the high-side machine to the high-side connected network, it will be marked with its appropriate classification.

7.7.5 Exceptions

There are no exceptions to equipment marking of the CI-100. If an occasion arises where the machines cannot be labeled, the using agency must request an exception through the ISSO and ISSM to the DAA.

7.8 Maintenance Procedures

7.8.1 General

All maintenance activities will be conducted on-site by personnel with at least a secret clearance and a need-to-know for the information passing through the CI-100. Routine maintenance (i.e., reviewing file transfer logs, etc.) will be conducted on a daily basis. In the event a patch or service pack must be installed, the configuration management procedures (subsection 7.5.3) will be followed. In the event of an after-hours maintenance requirement, on-call personnel will perform the maintenance provided they meet the clearance and need-to-know requirements.

Remote maintenance and diagnostic activities are not permitted. (Please see subsection 7.8.5.)

7.8.2 Uncleared Personnel

If an uncleared person is used to conduct maintenance on this system, a technologically-adept person will escort the person while in any area where classified information is used, discussed, or processed. All maintenance activity performed by this person will be noted in the maintenance logs. The escort requirement also applies if the maintenance person has a secret clearance but does not have a need-to-know for the information passing through the controlled interface.

7.8.3 Logs

The standard operating system logs will be maintained, and the ISSO will review them on at least a weekly basis or daily if a recurring problem is being monitored. These logs will audit the items listed in the SSP auditing subsections (i.e., subsections 7.6.5 and 7.6.6).

In the event a maintenance person is required to perform system administrator activities using another's user ID, a detailed log will be kept by the system administrator and ISSO noting the following items:

- The date and time of maintenance
- The user ID used to perform the maintenance
- The name and organization of the person performing the maintenance
- A description of the type of maintenance performed

7.8.4 Maintenance Software

Basic operating system maintenance software is used on the CI-100. Only a system administrator can perform certain maintenance activities. The operating system restricts access to this software.

7.8.5 Remote Diagnostics

Although it is strongly discouraged, the DAA may grant exceptions for the use of remote diagnostic software on the system. If granted, the diagnostic software will not be stored on CI-100 systems and will be kept in a locked container. A copy of the exemption will be maintained with this packet.

7.9 Sanitization and Destruction

7.9.1 Hardware

All sensitive and classified information is removed from all fixed media. The measures outlined in subsection 7.9.2 of this document are followed to sanitize the fixed media on the CI-100.

7.9.2 Data Storage Media

The destruction procedures for volatile memory are the same for any type of system. All power (direct and battery-provided) is removed from the memory chips. This causes all data stored on them to be destroyed. The quickest way to clear volatile memory is to turn off the computer, unplug it, and physically remove the memory chips from the motherboard.



b2
b7E

7.10 Software Security Procedures

7.10.1 Procurement

Software for the CI-100 will only be obtained through established FBI channels. Unless approved by the DAA, only software used in performing the OWT functions is permitted on the controlled interface. The program management office will test and approve new software for the interface prior to it being used on any of the devices.

7.10.2 Evaluation

Only approved software is permitted on the CI-100. The number of programs on the controlled interface is limited to only those programs that are needed to move data from the low security domain to the high security domain. If a system administrator wishes to install any additional software on the system, a request is submitted through the ISSO/ISSM to the DAA. The IAS will evaluate any security manifestations caused by the use of new software. The IAS and DAA must approve any software prior to it being installed on the system.

7.10.3 Malicious Code / Virus Protection

Up-to-date antivirus software will be used on the CI-100 to prevent an infection passing from the low side to the high side. The program must be properly configured so that in the event malicious software is detected, it isolates the offending packet(s) in the computer and permits the continued flow of data through the CI-100.

Under certain circumstances, viruses may be intentionally brought into the high-side network. In this event, the data owner will submit a statement acknowledging this fact to the DAA, and that statement will be included in the SSP for the classified network.

7.10.4 Data and Software Integrity Procedures



b2
b7E

7.11 Media Movement

7.11.1 Media Introduction and Removal Procedures

Due to its capabilities and limited functions, very few CI-100 associated removable media will need to be introduced into/taken out of the secure facility where the system is located. Only authorized removable media will be used in the CI-100 and will be procured through official FBI channels.

Classified media will be removed from the secure facility with the approval of the ISSO. For a period of five years, the ISSO will maintain documentation and statements as required pertaining to the:

- Justification for removal
- Approval/validation for removal
- Fact that the content was scanned/copied in accordance with the approved procedure
- Fact that the content of the data was reviewed by two technically qualified and authorized release individuals
- Verification that the process was monitored

7.11.2 Data Copying, Reviewing, and Releasing Procedures

The purpose of the CI-100 is to transfer information from an unclassified system to a classified system. Information processed by this controlled interface is not copied, does not need to be reviewed, and is not released while it is under the control of the CI-100.

7.12 Hardware Control

7.12.1 Transfer

To transfer a CI-100, the procedures for transferring classified information will be used. The CPU chassis will be double-wrapped in opaque material, the inner wrapping preferably being the computer carton. For specific instructions on transmitting/transferring classified information, see MIOG 26-7, *Transmittal of Classified Information*.

Prior to the transfer of the high-side computer, the hard drive will have all operational data removed from it. The hard disk will be overwritten in accordance with the procedures in subsection 7.9 of this document. The system can be used to process information at or above the classification of the data that it previously processed.

The ISSO will maintain a record for five years noting the:

- Justification for transfer
- Approval/validation for transfer
- Component was inspected in accordance with the approved procedure and written confirmation statement was provided
- Verification that the process was monitored
- Identity(-ies) of the person(s) performing these activities.
- The fact that all other non-volatile components may be released after successful completion of the procedures outlined in CSSM 130-2.

(S)

b1

7.12.2 Relocation

If the CI-100 is relocated, it must be placed in an area approved for processing the highest classification of the information passing across it. Additionally, a one-meter (39 inches) separation must be maintained when the system is relocated in the proximity of a lower classification system.

7.12.3 Release

If the CI-100 is to connect an unclassified network to a confidential/secret network and will be located in a sensitive compartmented information facility (SCIF), the hardware release procedures outline in DCI Directive 6/3 will be followed.

To release the low-side computer, the hard drive will have all programs and data removed from it. The hard disk will be overwritten in accordance with the procedures in SSP subsection 7.9 and then reformatted. The system can be used to process unclassified and above information.

To release the high-side computer, the hard drive will have all programs and data removed from it. The hard disk will be overwritten in accordance with the procedures in SSP subsection 7.9 and then reformatted. The system can be used to process information at or above the classification of the data that it previously processed.

The ISSO will maintain a record for five years noting the:

- Justification for release
- Approval/validation for release
- Component was inspected in accordance with the approved procedure and a written confirmation statement provided
- Verification that the process was monitored
- Identity (-ies) of the person(s) performing these activities

7.12.4 Maintenance

Properly cleared and trained FBI employees or contractors will maintain the CI-100. If this is not possible, a cleared non-employee or an uncleared person may conduct maintenance on the

system; however, a properly cleared, technologically-adept FBI employee or contractor will escort the person and supervise all work being done on the interface.

7.12.5 Introduction

If the CI-100 is to connect an unclassified network to a confidential/secret network and will be located in a SCIF, the hardware introduction procedures outlined in DCI Directive 6/3 will be followed.

If the CI-100 is located in a secret (collateral) area, new equipment will be introduced into the secure area with the approval of the ISSO and communications manager. Any new system must have been procured from a trusted source and if sent overseas, must remain under U.S. control from the time it leaves the United States until it arrives at the overseas office.

7.13 Web Protocol and Distributed/Collaborative Computing

Not applicable.

7.13.1 Web Server / Clients

Not applicable.

7.13.2 Mobile / Executable Code

Not applicable.

7.13.3 Collaborative Processes

Not applicable.

7.13.4 Distributed Processes

Not applicable.

7.14 Wireless Devices

Not applicable.

7.15 PKI Use

Not applicable.

8 SECURITY AWARENESS PROGRAM

8.1 Program Description

A security awareness program is currently being developed by Security Division and will be presented to all FBI employees and contractors.

8.2 Users' Guides

A basic system administrator manual is found in various sections and subsections of this SSP. In addition to this manual, each system administrator should maintain a Windows 2000 Professional/Server handbook.



9 INTERCONNECTION SECURITY AGREEMENT

If there are any interconnection service agreements, the ISSO will post them in this section.

10 MEMORANDA OF AGREEMENT

If there are any memoranda of understanding or memoranda of agreement, the ISSO will post them in this section.

11 AVAILABILITY

11.1 Restoration Procedures

Please refer to subsection 7.5.6 of this SSP.

11.2 Communications Back-up

A spare modified OWT cable (fiber optic or RS-232) will be maintained for each CI-100. In the event that the communications medium (the OWT cable) breaks, the spare can be quickly inserted. A spare fiber cable between the two fiber optic NICs on the low machine will also be maintained with the system.

In the event a NIC becomes inoperable, a replacement is modified, epoxied, and placed into the computer. The cable is connected to the NIC, and the computer is restarted.

11.3 Power Back-up

If the data owner, ISSO, and DAA representative agree that the CI-100 is a medium or high-availability system, the CI-100 will be connected to an uninterruptible power supply (UPS). If deemed appropriate, a program similar to APC's PowerChute may be installed to perform a graceful shutdown of the system, with the low side shutting down first, followed by the high side.

11.4 Denial of Service Prevention

The CI-100 is configured to accept data from a single computer on the unclassified network. Additionally, the CI-100 is not connected directly to the Internet and is located in FBI spaces. It is unlikely that it would be subject to an intentional denial-of-service attack. The ISSO and system administrators will monitor system and packet receipt logs to identify problems that may indicate the interface is being overloaded.

11.5 Priority Process Protection

In the CI-100, only a bare minimum number of processes are running. The reduced number of processes helps to prevent a lower priority process from interfering with a higher priority process.

Also, please see subsection 7.5.6. for the priority in recovery procedures.

12 EXCEPTIONS

There are no exceptions to policy for the CI-100. If one is needed, the following procedures will be used in the exception request.

Limitations in resources and technical capabilities may prevent the satisfaction of all security requirements without introducing unacceptable delay in achieving the operational requirements that the system was intended to satisfy. An *exception* indicates that the implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirement(s) may be used for a specified period of time. This is in contrast to a *waiver* that implies a security requirement has been set aside and need not be implemented at all. The DAA may authorize exceptions under the following conditions:

- Submission of a written request is submitted stating explicitly the requirements that are to be excepted and for what duration, including evidence of why the identified requirements cannot be implemented and indicating the countermeasures that are to be substituted
- Submission of a description of the aspect of the threat or associated vulnerability (ies) that is related to the proposed request and assurance that the consequent risk to the system will be acceptable based on other countermeasures that will be employed over the specified period
- Submission of a plan for implementing the “excepted” security requirements later in the system’s life cycle.

The procedures for requesting an exception to aspects of this SSP are:

- The data owner writes the business case (justification) for the exception to the SSP and provides it to the ISSO.
- The ISSO identifies possible risks introduced by this exception and provides existing or proposed risk mitigation measures.
- The ISSO forwards the packet to the ISSM.
- The ISSM, in conjunction with the Program Manager, evaluates the impact of the exception and proposed/existing countermeasures on the CI-100 and attached systems. The ISSM and Program Manager will make recommendations for additional safeguards or accepts the ISSO’s packet as is.
- The packet is forwarded to the DAA for consideration.
- If approved, the exception is processed under the configuration management program (Para. 7.5.3). Any changes to the CI-100 configuration must be issued by the configuration management board.

13 GLOSSARY OF TERMS

ABBREVIATIONS

CC Common Criteria
CM Configuration Management
CI Controlled Interface
DoS Denial of Service
ISA Interconnection Service Agreement
KVM Keyboard, Video, Mouse
MD Message Digest
MD5 Message Digest 5
NIST National Institute of Science and Technology

b1

(S)



NIC Network Interface Card
PDS Protected Distribution System
ssh Secure Shell
ssl Secure Sockets Layer
SANS SysAdmin, Audit, Network, Security Institute

DEFINITIONS

Checksum – (Please put definitions in this section.)

Configuration Management (CM) -

Controlled Interface (CI) -

Denial of Service (DoS)

Destruction

Hash

Interconnection Service Agreement (ISA)



High Side Computer

Keyboard, Video, Mouse (KVM)

Low Side Computer

Message Digest (MD) -

Message Digest 5 (MD5) -

National Institute of Science and Technology (NIST)

(S)



b1

Need-to-Know

Network Interface Card (NIC)

Overwrite

Protected Distribution System (PDS)

RS-232 --

Type Accreditation

RJ-45

Sanitization

Secure Shell (ssh)

Secure Sockets Layer (ssl)

SysAdmin, Audit, Network, Security Institute (SANS)

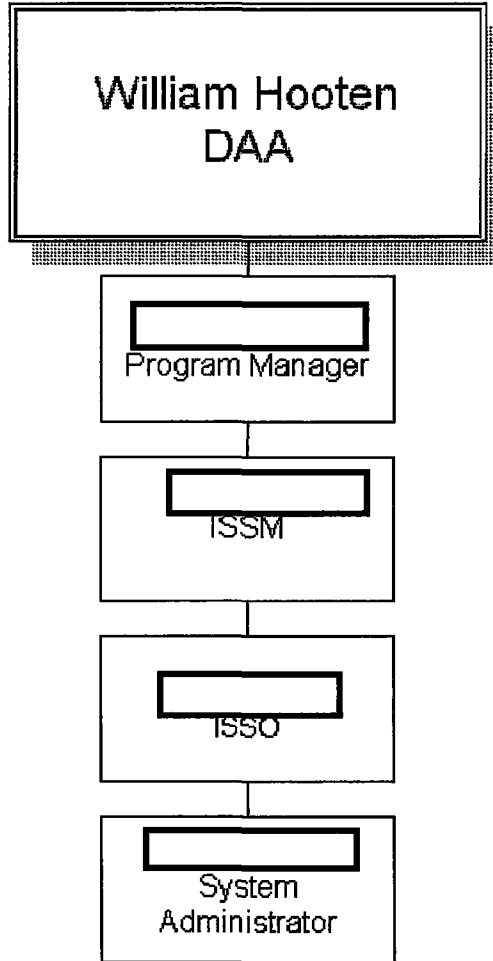
System Security Support Structure

Telnet

Threat

Vulnerability

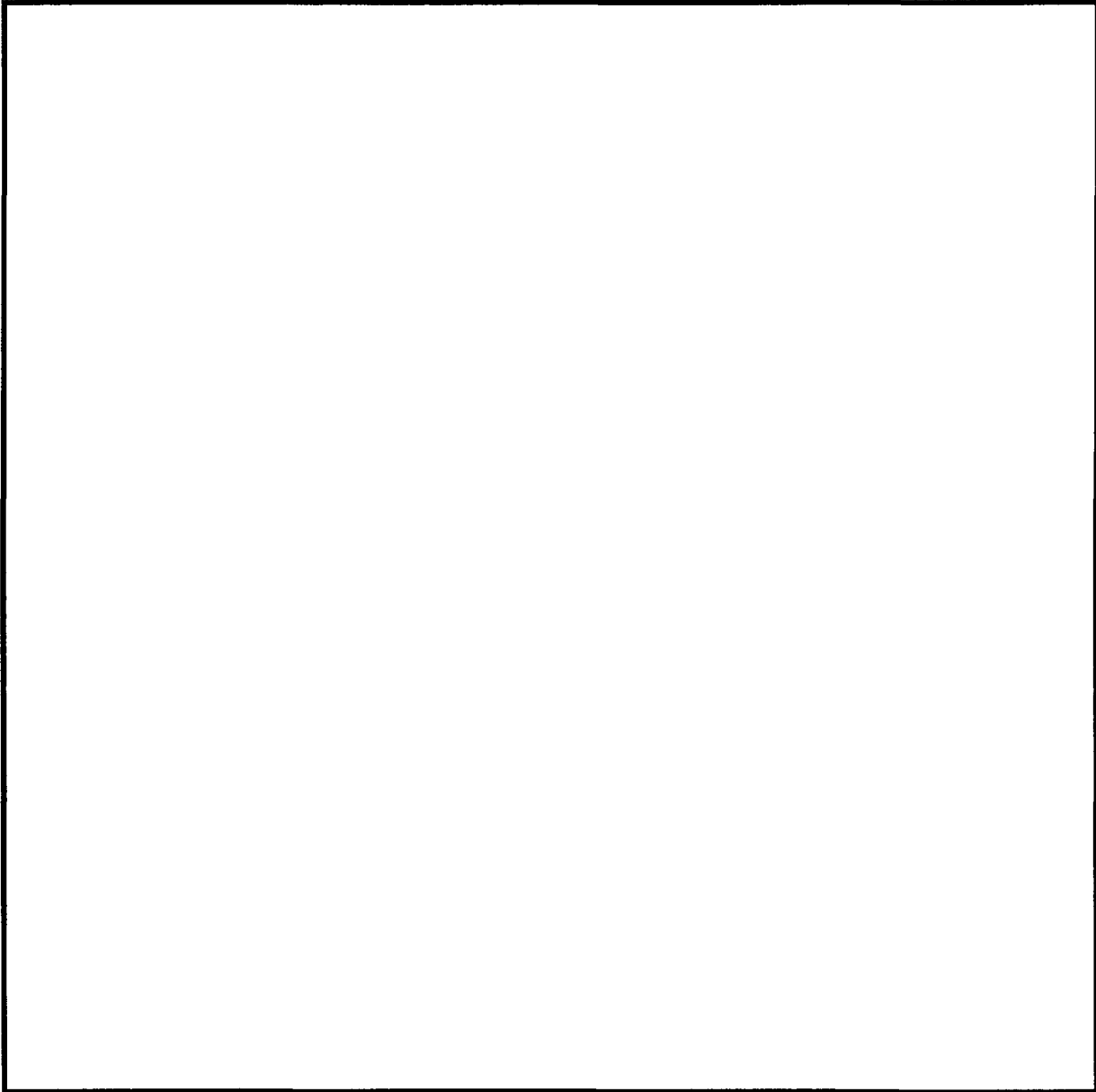
Appendix A - Organizational Structure



b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-19-2007 BY 65179/DMH/KSR/LMF

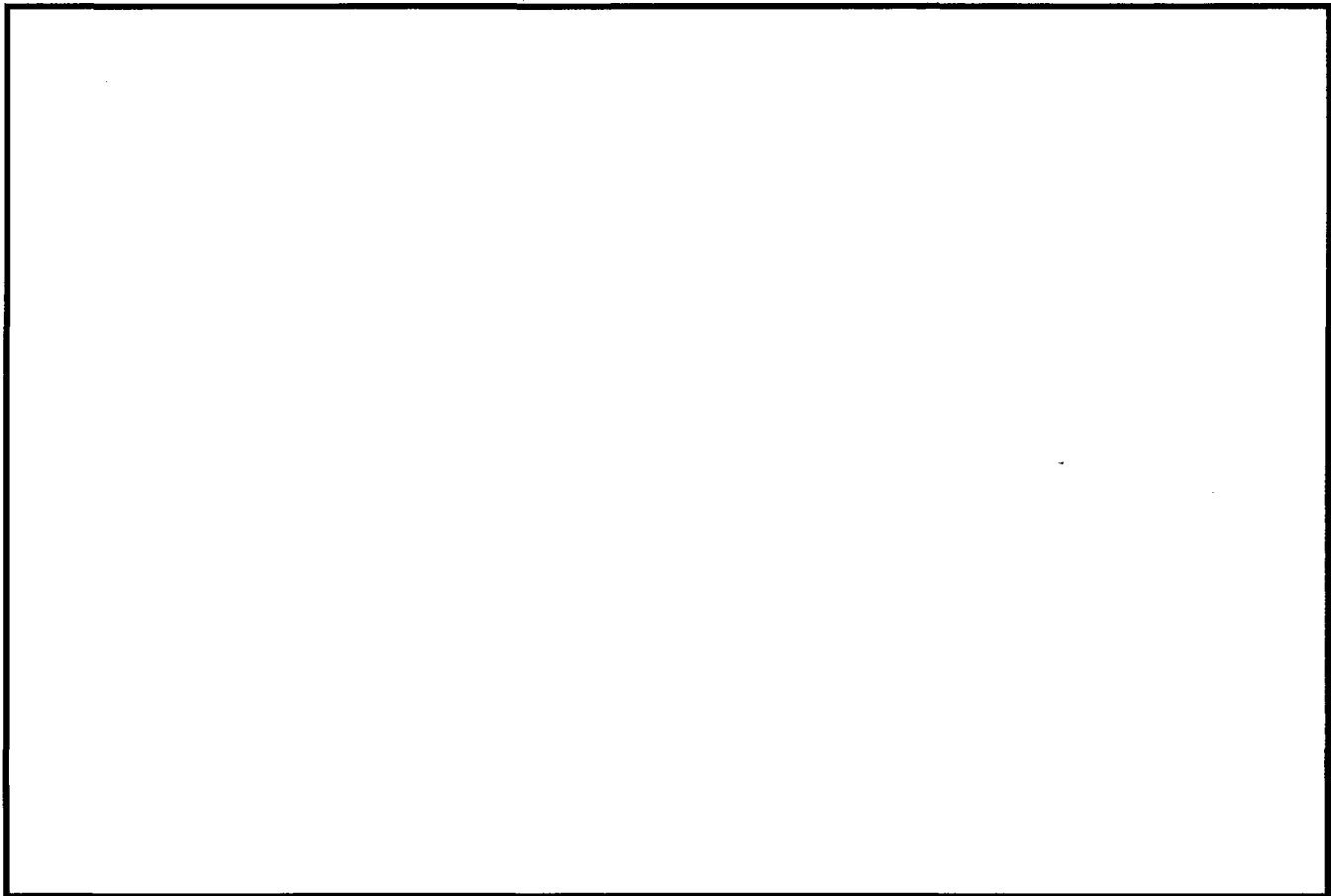
Appendix B - Facility Layout and Overview



b2
b7E

LIMITED OFFICIAL USE

Appendix C - System Equipment Location Floor Plan



b2
b7E

LIMITED OFFICIAL USE
PG-3

page 1



LIMITED OFFICIAL USE

Appendix D - System Handbooks

Appendix E - Risk Management Matrix

LIMITED OFFICIAL USE

Appendix F - Certification Test Plan and Results

LIMITED OFFICIAL USE
PG-5

~~page 1~~

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
	Table of Contents		P	
	Introduction		P	
1	Information System General Information		P	Added certifier and accreditation
1.1	Security Administration		P	
1.1.1	System Information	PL-2,SA-5	P	
1.1.2	Key System Points of Contact	AC-5,PS-2,SA-2	P	
1.1.3	Security Organization	AC-5,PS-2	P	
1.2	Mission		P	
1.2.1	Purpose and Scope	SA-5	P	
1.2.2	Supported Projects	SA-5	P	
1.2.3	Information System Usage	SA-5	P	
1.3	Inter-Departmental/Agency Use and Agreements		P	
1.3.1	Joint Use Information	CA-3,SA-5	P	
1.3.2	Memorandum of Agreement (MOA)/Understanding (MOU)	CA-3	P	
1.3.3	Interconnection Security Agreement (ISA)	CA-3	P	
2	Secure Facility Description		P	
2.1	Facility Layout	PE-1,PE-3	P	
2.2	Physical and Environmental Protection		P	
2.2.1	Physical Protection	MP-2,PE-1,PE-2,PE-3, PE-4,PE-5,PE-6	P	

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
2.2.2	Environmental Protection	PE-9,PE-10,PE-11,PE-12,PE-13,PE-14,PE-15	P	
2.3	System Layout	PE-2	P	
2.4	Emanation Protection		P	
2.4.1	Red/Black Separation	PE	P	
2.4.2	TEMPEST	PE	P	
3	System Description		P	
3.1	Summary	SA-5	P	
3.2	Protection Level/Mode of Operation	RA-2	P	SSP states Dedicated mode of operation should read System High Mode of operation
3.3	Levels of Concern		P	
3.3.1	Confidentiality	RA-2	P	
3.3.2	Integrity	RA-2	P	
3.3.3	Availability	RA-2	P	
3.4	Tier Designation	RA-2	P	
3.5	System Diagram	SA-5	P	
3.6	Interconnection Interface Description		P	
3.6.1	Direct Network Connection	CA-3	P	
3.6.1.1	Connectivity Management Procedures	CM-3	P	
3.6.1.2	Interconnection	CA-3	P	
3.6.1.3	Connectivity Procedures	CM-3	P	
3.6.1.4	Networking	CM-2	P	
3.6.2	Indirect Connections		P	
3.6.2.1	Indirect Import	SI-9,SI-10,SI-	P	

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
		11,SI-12		
3.6.2.2	Indirect Export	SI-13,SI-14	P	
3.7	Data Processed		P	
3.7.1	Classification and Compartments	RA-2	P	
3.7.2	Dissemination Controls	RA-2	P	
3.7.3	Type of Data Processed	RA-2	P	
3.8	Data Flow Diagram	SA-5	P	
4	System Hardware		P	
4.1	Hardware List	CM-2,SA-5	P	
4.2.1	Labeling of System Hardware	MP-3	P	
4.2.2	(System Hardware) Exceptions	MP-3	P	
4.3	Sanitization and Destruction	MP-6,MP-7	P	
4.4	Custom-Built Hardware	CM-2,SA-5	P	
5	System Software		P	
5.1	Software List	CM-2,SA-5	P	
5.2	Software with Restricted Access or Limited Use Requirements	CM-2,SA-5	P	
5.3	Foreign Software	CM-2,SA-5	P	
5.4	Freeware/Shareware/Open-Source Software	CM-2,SA-5	P	
5.5	(System Software) Marking and Labeling	MP-3	P	
6	Data Storage Media		P	
6.1	Media Type	CM-2,SA-5	P	
6.2	Media Handling	MP-2,MP-4,MP-5	P	
6.2.1	Media Introduction and Removal	MP-2	P	

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
6.2.2	Sanitization and Destruction	MPMP-6,MP-7	P	
6.3	Storage Media Marking and Labeling	MP-3	P	
7	Security Control Requirements		P	
7.7.1	Risk Assessment	RA-1,RA-3,RA-4	P	
7.1.2	Compliance and Monitoring Program	CA-7,CM-4,IR-5,PE-6,RA-4,RA-5	P	
7.2.1	Personnel Security	PS-1,PS-2,PS-3,PS-4,PS-5,PS-6,PS-8	P	
7.2.1.1	Non-US Citizens	PSPS-3,PS-6,PS-7	P	
7.2.2	Contingency Planning		P	
7.2.2.1	System Backup	CP-9	P	
7.2.2.1.1	Backup Protection	CP-6	P	
7.2.2.1.2	On-site & Off-site Storage	CP-6	P	
7.2.2.2	Telecommunications Services	CP-8	P	
7.2.2.3	Backup Power Supply Requirements	CP-2,PE-11	P	
7.2.2.4	Recovery Procedures		P	
7.2.2.4.1	Continuity of Operations Plan	CP-2,CP-5	P	
7.2.2.4.2	Disaster Recovery Plan	CP-10	P	
7.2.3	Configuration Management Program	CM-1,CM-2,CM-3,CM-4,CM-5	P	
7.2.3.1	Hardware & Software Procurement	CM-2,CM-3	P	
7.2.3.2	Evaluation	CM-3,CM-4	P	

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		P	
7.2.4.1	Maintenance and Repair Procedures	MA-1,MA-2,MA-6	P	
7.2.4.2	Maintenance Procedures Using Uncleared Personnel	MA-5	P	
7.2.4.3	Maintenance Logs	MA-1	P	
7.2.4.4	Hardware & Software Maintenance		P	
7.2.4.4.1	System Start-Up/Shut-Down	MA-1	P	
7.2.4.4.2	Security Controls and Operations During Maintenance	MA-1	P	
7.2.4.4.3	Remote Diagnostics	MA-4	P	
7.2.4.4.4	Hardware & Software Transfer, Relocation, and Release	MA-3	P	
7.2.5	System & Information Integrity		P	
7.2.5.1	System Integrity		P	
7.2.5.1.1	System Start-up	SI-1	P	
7.2.5.1.2	After Hours Processing Procedures	SI-1	P	
7.2.5.2	Data and Software Integrity		P	
7.2.5.2.1	Data and Software Integrity Procedures	SI-7	P	
7.2.5.2.2	Data Copying, Reviewing, and Release Procedures	SI-9,SI-10,SI-11,SI-12	P	
7.2.5.2.3	Printout/Hardcopy	SI-12	P	
7.2.5.2.4	Non-Repudiation	SC-17	P	
7.2.5.2.5	Transaction Rollback	CP-9,CP-10	P	
7.2.6	User's Guides		P	
7.2.6.1	Configuration Guides	PL-2,SA-5	P	
7.2.6.2	Guides for Privileged Users		P	

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		P	
7.2.7	Incident Response	AU-6,AU-7,CA-7,IR-1,IR-4,IR-5	P	
7.2.7.1	ISSO Notification during Suspicious Events	AU-6,AU-7,IR-7	P	
7.2.7.2	Actions Taken By System During Suspicious Events	IR-4	P	
7.3	Technical		P	
7.3.1	Access Control		P	
7.3.1.1	Discretionary Access Control (DAC)	AC-1,AC-3,AC-6,AC-10,AC-13	P	
7.3.1.1.1	Need-To-Know Controls	ACAC-3,AC-4,AC-6	P	
7.3.1.1.2	Discretionary Access Control Augmentation	AC-4,AC-6,AC-15,AC-16	P	
7.3.1.2	Mandatory Access Controls (MAC)	AC-4,AC-13,AC-15,AC-16	P	
7.3.1.2.1	Internal Marking and Labeling	AC-15,AC-16	P	
7.3.1.3	Technical Access Control Mechanism	AC-3,AC-11,AC-12,AC-14	P	
7.3.1.4	User Group and Access Rights	ACAC-5,AC-6,AC-14	P	
7.3.1.4.1	User Groups	AC-2	P	

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	AC-2,AC-5	P	
7.3.1.4.1.2	General User Group Roles	AC-2,AC-5	P	
7.3.1.4.2	System Access Rights		P	
7.3.1.4.2.1	Local System Access Rights	AC-3	P	
7.3.1.4.2.2	Remote System Access	AC-17	P	
7.3.1.4.2.3	Non-Data File Access	AC-3	P	
7.3.1.4.3	Privileged Users Access Rights	AC-3,AC-5,AC-6	P	
7.3.1.5.1	Log-On Error Handling		P	
7.3.1.5.1	Log-on Error Handling	AC-7	P	
7.3.1.5.2	Account Lockout Handling	AC-7	P	
7.3.2	Identification & Authentication	IA-1	P	
7.3.2.1	System Users		P	
7.3.2.1.1	General Users	IA-2	P	
7.3.2.1.2	Privileged User	IA-2	P	
7.3.2.1.3	Device/System User	IA-2	P	
7.3.2.2	Account Management Procedures		P	
7.3.2.2.1	Account Request Procedures	AC-2	P	
7.3.2.2.2	Account Maintenance Procedures	AC-2,IA-4,IA-5	P	
7.3.2.2.3	Account Termination Procedures	AC-2	P	
7.3.2.3	Authenticator Procedures	IA-5	P	
7.3.2.3.1	Password Generation	IA 5	P	
7.3.2.3.2	Password Changes	IA-5	P	
7.3.2.4	PKI Use	IA-7	P	
7.3.2.5	Trusted Multi-Level Communication Path	SC-11	P	
7.3.3	Accountability (Including Audit		P	

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	AU-1	P	
7.3.3.1.1	Audit Review	AU-6	P	
7.3.3.1.2	Audit Log Storage Requirements	AU-4	P	
7.3.3.1.3	Discrepancy Handling	AU-5	P	
7.3.3.1.4	System Shutdown During Audit Failure	AU-5	P	
7.3.3.2	Notification Banner	AC-8	P	
7.3.3.3	User Accountability	PS-6	P	
7.3.3.4	Audit Protection and Log Access		P	
7.3.3.4.1	Audit Protection	AU-9	P	
7.3.3.4.2	Audit Log Access	AU-9,AC-3	P	
7.3.3.5	Audited Information	AU-3	P	
7.3.3.5.1	Windows Operating System		P	
7.3.3.5.2	Solaris Operating System		P	
7.3.3.5.3	Oracle Database		P	
7.3.3.5.4	Microsoft SQL Database		P	
7.3.3.5.5	Microsoft Internet Information Server (IIS)		P	
7.3.3.6	Audited Activities	AU-2	P	
7.3.3.6.1	(Audited Activities) Windows Operating System		P	
7.3.3.6.2	(Audited Activities) Solaris Operating System		P	
7.3.3.6.3	(Audited Activities) Oracle Database		P	
7.3.3.6.4	(Audited Activities) Microsoft SQL Database		P	

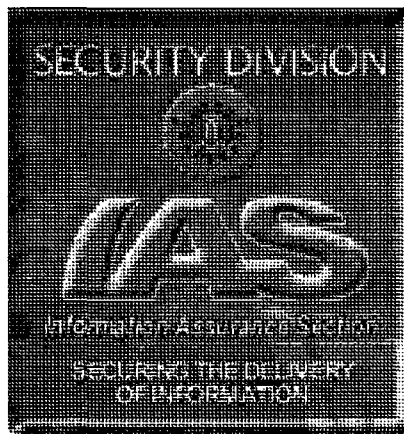
DCS 3000] System Security Plan (SSP) v3.0 dated 04/28/2006
Errata Sheet – [05/23/2006]

Page/Section/Paragraph	Title	SRTM	Pass/Fail	Comments
7.3.4	System & Communications Protection		P	
7.3.4.1	Systems Protections	SC-1,SC-2,SC-3	P	
7.3.4.1.1	Malicious Code/Virus Protection	SC-18,SI-3,SI-8	P	
7.3.4.1.2	Denial of Service Protection	SC-5	P	
7.3.4.1.3	Priority Process Protection	SC-6	P	
7.3.4.2	Communications Protection	SC-1	P	
7.3.4.2.1	Network Allowed Services and Protocols	SC-7,CM-2,CM-6,CM-7	P	
7.3.4.2.1.1	Internal to the LAN:		P	
7.3.4.2.1.2	External to the LAN:		P	
7.3.4.2.2	Controlled Interface Requirements	SC-7	P	
7.3.4.2.2.1	Controlled Interface to System #1		P	
7.3.4.2.2.2	Controlled Interface to System #2		P	
7.3.4.3	Unique Security Features	SC-12,SC-13,SC-16,SC-17,SC-19	P	
7.3.4.3.1	Mobile/Executable Code	SC-18	P	
7.3.4.3.2	Collaborative Processing	SC-15	P	
7.3.4.3.3	Distributed Processing	SC-4	P	
7.3.4.3.4	Wireless Devices	AC-18,SC-8,SC-9	P	
8.1	(Security Awareness Program) Program Description	AT-1,AT-2,AT-3,AT-4	P	

**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	PS-6	P	
9	Exceptions		P	
10	Glossary			
Attachments				
A	Organizational Structure		P	
B	Detailed System Diagram or System Security Architecture		P	
C	Facility Layout and Overview or System Equipment Location Floor Plan		N/A	Multiple floor plan system deployed to 80 cites
D	Equipment List			
E	Software List			
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)			


Executive Summary Validation of System Mitigation Actions Security Test Report



DCS3000

May 26, 2006

b6
b7C


Certification Unit
Information Assurance Section
Security Division

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-05-2007 BY 65179DMH/KSR/LMF

INTRODUCTION

On 2 May 2006 Accreditation Unit requested the Certification Unit to validate the eight (8) findings documented in the DCS-3000 Risk Management Matrix (RMM), dated 5 November 2002. The request for Certification validation is to ensure that eight findings have been properly mitigated by the system owner (Telecommunications Intercept and Collection Technology Unit (TICTU)). The results of the Certification validation is incorporated in the DCS-3000 Exective Summary Report in order to facilitate the decision by the accreditor to re-accredit the system for an additional three (3) years.

The Enterprise Security Operations Center (ESOC) assisted Certification Unit by the security evaluation of the DCS-3000 in accordance with the C&A handbook section 3.7.7.2 and Appendix C. The objective of the testing were to identify if proper actions were applied to mitigate the eight (8) vulnerabilities identified in the DCS-3000 RMM.

This report documents the results of the May 26, 2006 testing performed by the ESOC on the DCS3000 located in the FBI Engineering Research Facility (ERF).

USE OF OPERATIONAL DATA & CONNECTIVITY REQUIREMENTS

The DCS-3000 system is classified as Sensitive But Unclassified (SBU) and operational and deployed in central monitoring plants (CMP) located in FBI field offices and at the FBI Engineering Research Facility (ERF). ESOC performed testing on the ERF DCS-3000 only. Testing on the other DCS-3000 type systems at other Field Offices locate throughout the country was not part of this testing scope. Further testing by the ISSM/ISSO on other DCS3000 type systems at other Field Office facilities is still required to ensure they are the same configuration as the tested system at the ERF.

SECURITY TESTING APPROACH

Security testing is conducted within the scope of the objectives described above. All validation testing scenarios performed were manual inspection of the DCS-3000 system located in the ERF facility.

b6

b7C

TEST SUMMARY

ESOC Vulnerability Assessment Test Team Member, was designated and performed validation testing of the eight (8) vulnerabilities identified

in the DCS3000 RMM, dated November 5, 2002. The only system tested was the DCS3000 located in ERF, Quantico.

FINDINGS¹

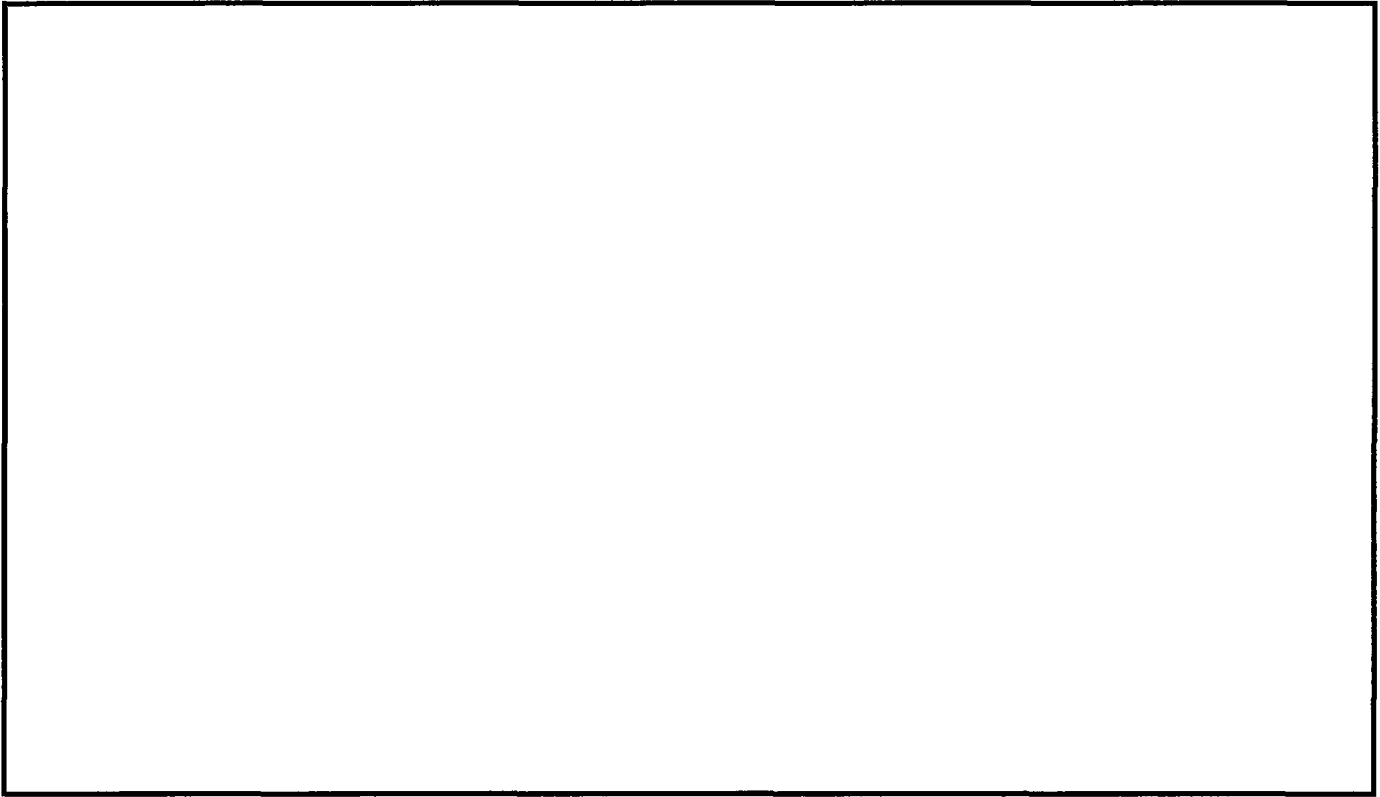
Table 1 documents the results of the validation testing performed by ESOC on 26 May 2006. Based on the ESOC findings, six (6) of the eight (8) findings have been verified as mitigated. One finding, "Improper workstation permissions," was a false finding based on the DCS-3000 SSP, dated April 28, 2006, Section 7.3.14.1. This sections states, "The DCS-3000 utilizes a single user class with administrative rights for all ELSUR operations." Based on that Accreditor approved SSP, least privileges on the workstation based on roles is not required. The only other vulnerability identified that has not been mitigated is finding # 8, Lack of Intrusion Detection Systems (IDS). ESOC has verified that this vulnerability is still active and has not been mitigated by the system owner.

Table 1 – Validation Results

b2
b7E

DCS3000 VALIDATION RESULTS			
Finding #	Vulnerability	Severity	Mitigation
1.	No anti-virus software found. VL = High	HIGH	Methods to be used to limit the risk: - Install FBI approved anti-virus software on all servers and workstations. - System administrators ensure all virus signatures are updated weekly or as needed. RR = Low Verified McAfee 4.5.1 installed with Virus updated 05/05/2006
2.	Insufficient password management controls VL = High	HIGH	Recommend enforcing mandated password policies. As a minimum: <div style="border: 2px solid black; height: 60px; width: 100%;"></div> RR = Low Verified
3.	Insufficient account lockout policy VL = High	HIGH	Recommend instituting an account lockout policy by implementing, at a minimum: - Account lockout duration - Account lockout threshold (i.e. 3 attempts) - Unlock procedures RR = Low Verified Accounts lock out after three attempts and must be reset by admin.

DCS3000 VALIDATION RESULTS			
Validation ID	Severity	Findings/Recommendations/Remediation	Notes/Status
4. Inadequate audit logging. VL = Medium	MEDIUM	Recommend implementing workstation and server auditing and log dumps on a daily basis to reduce impact on resources. RR= Low	Verified Routers syslog and systems event viewer is set to record all events.
5. Improper workstation permissions. VL = High	HIGH	Recommend the implementation of workstation permissions to give least privilege access. RR= Low	Failed Software required to run with admin privileges. See SSP.
6. Improper guest/administrator account configuration. VL = High	HIGH	Recommend deleting the guest accounts and renaming the administrator accounts. RR = Low	Verified Guest account is disabled and the Administrator account is renamed.
7. Lack of Intrusion Detection Systems (IDS) VL = High	HIGH	Recommend implementing an intrusion detection scheme. RR = Low	Failed No IDS is installed.
8. Telnet login is not encrypted VL = High	HIGH	Recommend a secure Telnet implementation. RR = Low	Verified Telnet is not being used.



b2
b7E

DCS-3000 Accreditation Boundary

PG-5

FEDERAL BUREAU OF INVESTIGATION

Precedence: Immediate

Date: 05/31/2006

To: Security

Attn: [Redacted]

From: Security

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

Contact: [Redacted]

b6
b7C

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 Intrusion Detection System (IDS), has not been corrected or mitigated.

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

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

PG-3

LIMITED OFFICIAL USE ONLY



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

August 27, 2002

Prepared by:
Certification Test Team



b6
b7C

LIMITED OFFICIAL USE ONLY

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-19-2007 BY 65179/DHR/KSR/LMF

PG-1

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

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

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

1.0 PRE-CERTIFICATION TEST RESULTS

(U) The test results reported herein were generated as part of a pre-certification test effort. The purpose of this set of tests is to allow the system provider to make security-related modifications to the DCS 3000 system prior to the main certification testing effort. The format of this document is based on that used for Appendix F of the System Security Authorization Agreement (SSAA).

~~(S)~~ Based on the certification review of the DCS 3000, several significant information assurance deficiencies were found. (U) These findings are based on document review, interviews of both system administrators and users, and actual testing.

(U) Since time limits prevented thorough testing of the DCS 3000, a sufficient sampling was made to draw conclusions about practices, capabilities and deficiencies. Tests were performed in priority order taking account the sensitivity of information contained therein and the importance for immediate continuity of the system in a time of crisis.

~~(S)~~ The major deficiencies were in the areas of passwords and permission (access controls).

(U) All of these deficiencies indicate a lack of proper infrastructure for the information assurance of the DCS 3000. Some of these are a direct result of the certification testing, and others are a result of interviews with both users and system administrators as well as review of existing documentation.

1.1 Testing Constraints

(U) Security should ensure that procedures, policies, and practices are in place to ensure data confidentiality, integrity, and operational availability of the DCS 3000.

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~F-1~~

LIMITED OFFICIAL USE ONLY

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) With the exceptions noted in the Section 3.0, all tests were performed in the test environment. In addition to the certification and accreditation team members present at the tests, test team participants included the CSSO, technical project manager and program sponsor. Test dates and participants are listed in Section 2.0 of this document.

1.2 Major Findings

(U) Numerous findings have been identified for the DCS 3000. These fall into both the technical and the policy/procedural areas. The following sections summarize the major findings.

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

(U) Suggestions for mitigating changes are included in several finding descriptions. The system owner/administrator must assume full responsibility for making such changes correctly. Before making any changes, the system components should be completely backed up. The suggested changes should be researched to determine if there are more current fixes available. Caution is advised as to the proper order in which the changes are made, as they are usually not independent of each other. Finally any changes should be made in compliance with current configuration management guidelines.

(U) The following tables briefly summarizes the technical findings:

1.2.1 Technical Findings

~~(U)~~ The following table briefly summarizes the technical findings. These findings are serious and numerous.

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~F-2~~

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

No.	Major Security Findings	Test Case	Scan Report
DISA SRR OS Scan			
(U) 1.	X	VS-03	Audit.Txt
(U) 2.		VS-03	Files.Txt
(U) 3.		VS-03	Registry.txt
(U) 4.		VS-03	Accounts.txt Users.txt
(U) 6.		VS-03	Users.txt

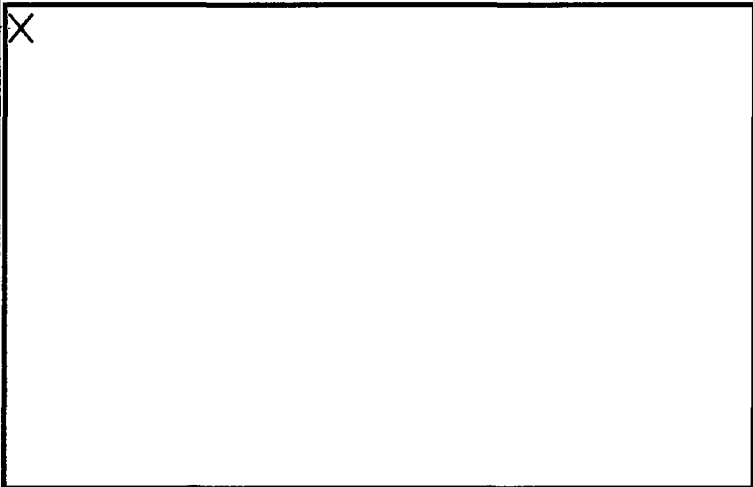
b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
1	ISS System Scanner 	VS-01	Workstation Vulnerability Report page 1

(U)

b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
2	X	VS-01	Pages 3-5, 7, 20, 26 of Workstation Vulnerability Report .

(U)

b2
b7E

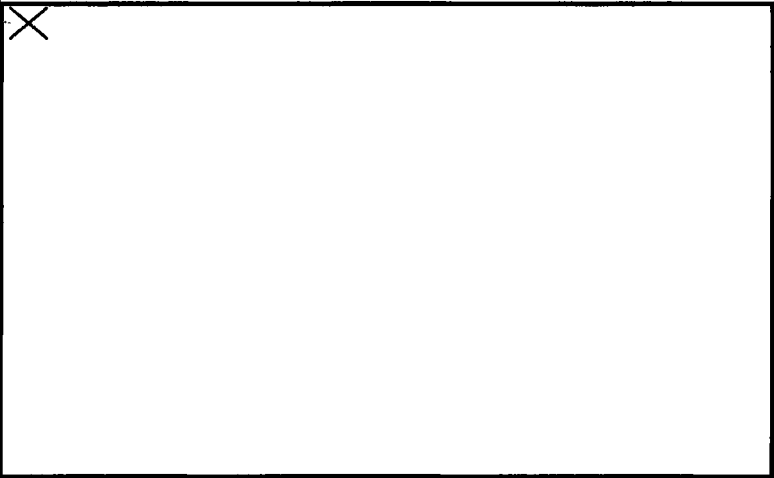
August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U)

No.	Major Security Findings	Test Case	Scan Report
3.		VS-01	

b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

No.	Major Security Findings	Test Case	Scan Report
(U) 4	X	VS-01	Pages 2- 3 of Workstation Vulnerability Report . b2 b7E

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

CISCO Secure Scanner			
(U) 1	X	NS-CS-01	CSS Vulnerability Report
(U) 2	X	NS-CS-01	CSS Vulnerability Report

b2
b7E

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Operating System Manual Testing			
(U)	1. X	SI-03	Refer to page 23 of this document.

1.2.2 Procedural/Policy Findings

b2
b7E

(U) The following list identifies the policy and procedural findings:

Not tested in pre-certification test..

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

2.0 TEST SCHEDULE

(U) Testing was scheduled to occur between August 22, 2002 and August 23, 2002. Data entry, analysis and final editing of this document occurred between August 27, 2002 and August 31, 2002.

(U) The following table lists the test script groups and the dates that testing, results recording and analysis was completed for that group.

(U)

Test Script And Result File	Testing Completed	Results Recorded	Analyses Completed
DISA Windows 2000 SRR scripts	8/22/02	8/27/02	
ISS Vulnerability Scan (System)	8/23/02	8/27/02	
CISCO scanner software	8/23/02	8/27/02	

August 27, 2002



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

3.0 TECHNICAL TESTS AND TEST RESULTS

(U) The following pages describe the actual tests performed. The tests are grouped as in the previous table. The order of the groups is essentially the sequence in which they were performed.

(U) Each test case includes a Test Description, the relevant Requirements, the desired Test Preparation, a table of Test Procedures and Results, and Analysis of Results, and finally a Pass/Fail table.

(U) Several test cases used automated vulnerability scanner test scripts. The results of these scans provide the detailed vulnerabilities, i.e., those specific items that must be fixed by modifying the system or determining the history of prior changes. These detailed results are the basis for several of the major findings reported herein. They are not included in this document, as they are directed towards system administrators whose job it will be to make the DCS 3000 adequately secure. However, they are available on request. They include:

- 1) (U) Security Readiness Review (SRR) scripts, Windows 2000 test results and findings
- 2) (U) ISS System Scanner test results and findings
- 3) (U) CISCO SYSTEM scanner test results and findings
- 4) (U) Manual test scripts and findings

BANNERS AND LABELS TEST SCRIPTS AND RESULTS

(U) Test Case BL-01: Test for Standard Security Warning Banner

(U) Description: This test determines if the standard security warning banner appears prior to login on both servers and workstations.

(U) Preparation: The system administrator shall send a system alert message to all users to save work and logout to allow testing. All workstations attached to the system network must be powered-up. They should not be logged on.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Press CTRL+ALT+DELETE keys to unlock the console (if locked) and to initiate the login process on the Primary Domain Controller. Login using a valid user ID and password. Logout and lock console. For each of a sample of workstations using an NT-based operating system in several locations, power up and press CTRL+ALT+DELETE to initiate the login process. Login using a valid user ID and password. Look for the warning banner. Shutdown.	Standard warning banner should appear at a point prior to login.	8/23/02	As expected (The standard FBI banner does exist.)

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Pass/Fail:

Requirement	Pass/Fail	Comment
(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."	Pass	

**System Security Plan (SSP)
DCS 3000**

Pre-Certification Test Results and Findings

(U) Test Case BL-02: Verifying Hardware has Proper Government Property Tags and Labeled with Proper Security Labels

(U) **Test Description:** This physical inspection checks for the existence of appropriate security labels affixed to hardware.

(U) **Test Preparation:** None.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	All System equipment shall be examined for the proper security label.	Hardware processing, transmitting or storing data should have be labeled at the highest security level of the data handled.	8/23/02	As expected.
2	Review procedures for handling hard disk drives from system hardware, either for destruction or transfer.	Must be handled only by FBI personnel and not leave controlled facility, as per requirements. System maintenance staff must be aware of and follow such procedures.	8/23/02	As expected.

(U) Pass/Fail:

Requirement	Pass/Fail	Comment
(U) MIOG 35-9.4.10(1)(a): All systems with non-removable ADPT storage devices must conspicuously display classification and data descriptor labels on the unit that contains the magnetic ADPT storage device. The monitor may also be labeled.	Pass	

August 27, 2002

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	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) **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.

(U) Test Description: Confirm that removable media has the proper SF-707 classification and data descriptor labels. Examine diskettes, CDs, back-up tapes. Confirm that there are procedures in place to address the disposal of fixed and removable magnetic media, hard copy and printer ribbons. Confirm that backup media and installation are properly labeled as to date, and properly protected. Examine storage area.

(U) Test Preparation: None.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	The SA shall confirm that removable media has the proper SF-707 classification labels attached to removable media through spot checks.			Not applicable.
2	Check for documented procedures for disposal of hard Copy/Magnetic Media.			Not applicable.
3	The SA shall show room location and storage location of backup media.		8/23/02	As expected.

(U) Pass/Fail:

August 27, 2002

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.		N/A
(U) MIOG 35-9.4.14(1)(e) : 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.		N/A
(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.	Pass	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Test Case BL-04: Data Record Marking

(U) Description: This test contains several tests to determine if the means exist to effect a page or record labeling mechanism for security markings.

(U) Preparation: None

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Review data dictionaries for the Oracle database application tables to determine if required security marking fields are included.	Fields are included on the data dictionaries.		N/A
2	Review a sample of records from the Oracle database application to determine whether the security marking fields are populated appropriately.	Sample shows that fields are populated appropriately.		N/A

SYSTEM INTEGRITY TEST SCRIPTS AND RESULTS

(U) Test Case SI-01: Test for Anti-Virus Protection

(U) Description:

This test determines if then necessary preparations have been made to protect the system from viruses. This includes having current virus signature data.

(U) Preparation:

The system administrator shall be able to verify existing anti-virus mechanisms.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	The SA shall log onto each workstation among the sample allocated for this purpose, as administrator, and open the anti-virus protection program. Observe what resources are scanned, and the frequency at which automatic scans are performed, and at what level of detail, e.g., executables, files, boot sector.	All floppy disk volumes must be scanned when mounted. The boot sector, and key system files should be scanned on startup. Detailed scanning of all files should occur at least weekly at a designated time that has the least impact on work productivity.	8/23/02	Fail No anti-virus software was found.
2	The SA shall determine on each selected workstation, the date of the virus signature data file(s) in place.	They should not be more than one week older than the latest available from the vendor.	8/23/02	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

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
3	Verify procedures used upon detection of virus or other malicious software.	Procedures must be written and well-understood by all system users.	8/23/02	Fail. Presently, there are no virus checking programs in place

(U)

~~(S)~~ Pass/Fail:

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**

(U) Test Case SI-02: Verifying System Data and Program Backup and Restore

Test Description:

This test determines the extent to which system backup and restore are operational.

Test Preparation:

None.

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Review back-up job streams used to perform to determine if all software and data is included in the backups.	All data and software should be backed up.	8/23/02	According to [redacted] backups are handled centrally by FBI on FBINET.. b6 b7C
2	Determine where backup media are stored.	Media should be stored in a secured location. Periodically, complete backup media must be stored at an off-site location.	8/23/02	According to [redacted] backups are handled centrally by FBI on FBINET.
3	Determine if it is possible to restore to a computer with lower security protection.	No computer with drives capable of reading the backup media should be co-located with the system that is cleared to a lower security level.	8/23/02	As expected.

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Pass/Fail:

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	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Test Case SI-03: Verifying System Integrity Safeguards

(U) Test Description:

This test determines the extent to which system integrity safeguards are in place.

(U) Test Preparation:

None.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Verify that access to update source code is limited to specified programmers. Application user should attempt to update application source code.	Access to update the source code should be limited to two persons.	8/23/02	As expected

(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	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Test Case SI-04: Verifying System Software Licenses

(U) Test Description:

This test determines the extent to which commercial software used on the system is licensed.

(U) Test Preparation:

The system administrator or program manager shall produce documented evidence of licences for commercial software used on system.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Verify all installed software is properly licensed.	All licenses are current and available	8-23-02	As expected.

(U) Pass/Fail:

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	

August 27, 2002

NETWORK CONNECTIVITY TEST SCRIPTS AND RESULTS

(U) Test Case NC-01: Intranet Connectivity

(U) Test Description:

This test determines if any Internet or intranet sites outside the system can be accessed from the system workstations. The first steps test if the system and other intranet computers can be reached via simple TCP/IP commands. This test is performed using all workstation operating systems.

(U) Test Preparation:

Test user accounts shall have been created. The systems administrator shall provide the IP addresses of the Primary Domain Controller. Test team will need IP addresses outside the network to ping.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	The SA shall, on several workstations for each workstation operating system, attempt to use the TCP/IP Ping command to determine if the System PDCs will respond. On Windows workstations, the MS-DOS window or the Run Command may be used.	The PDC of the operational portion of the System should respond with several lines giving timing information. The ping command to the PDC on the test portion of the System should time out.	8/23/02	N/A The intranet was not used.
2	The SA shall, on at least one workstation for each workstation operating system, attempt to use the Ping TCP/IP command to determine if computers having selected sites assumed to be outside the network respond.	No non-System site should respond, and the ping commands should time out.	8/23/02	N/A.

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
3	Using the workstation Web Browser, attempt to open the home pages for the browser vendor (these should be available in the setup options for the browser.)	Attempts should fail.	8/23/02	N/A.
4	All System personnel shall be asked to log onto the System using their own account Usernames and passwords. Inspect directories that contain cookies, and addresses of sites visited, for outside locations.	No non-System site locations should be referenced.	8/23/02	N/A.

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Pass/Fail:

Requirement	Pass/Fail	Comment
<p>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.</p>	<p>N/A</p>	
<p>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.</p>	<p>N/A</p>	

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) **Test Case NC-03: Verifying Physical Connections**

(U) Test Description:

This test looks for undocumented maintenance ports, modems. No connectivity outside the network is expected.

(U) Test Preparation:

Electronic technicians to provide access to wiring closets, as required, to provide available wiring diagrams, and equipment for continuity testing and line-loss measurement. Wiring diagrams and installation line loss values shall be made available.

(U) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	The SA/ET staff shall physically verify each wire connection beginning with the servers continuing through switches, hubs to each termination point, verifying cable numbers and ports.	There should be accountability for each connection as described on the network diagram.	8/23//02	As expected.
2	Line continuity tests shall be made to verify correct cable connections and labeling. Line loss measurements shall be made to determine if a possible splice or break exists. Comparisons with documented line loss shall be made when installation values are available.	Cables should be connected and labeled according to documentation. Line loss shall not indicate splice or break in line continuity.	8/23/02	As expected.

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Pass/Fail:

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	

NETWORK VULNERABILITY SCANNER TEST SCRIPTS AND RESULTS

(U) **Test Case NS-01: Identify network vulnerabilities using Cisco Security Scanner (CSS)**

(U) Features of the CSS scanner:

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

The Cisco Security Scanner is a network-based security assessment tool. It provides extensive port and service scanning and network vulnerability analysis. It can perform scheduled and selective probes of network devices including routers and switches, networked hosts, operating systems and key applications. During a scan, it identifies a comprehensive set of vulnerabilities likely to be exploited during network attacks, and recommends corrective action. CSS prepares reports and data sets to support policy enforcement.

(U) Description:

This test runs the CSS Security Scanner vulnerability assessment tool. General features are described above. This test targets network vulnerabilities.

(U) Preparation:

The Certification Test Team shall provide the CSS scanner with the latest vulnerability signatures. The System Administrator (SA) shall install the CSS scanner where needed.

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(?) Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Install Cisco Security Scanner on NT4 Server.	Application should install properly.	8/23/2002	As expected
2	Execute the scanner tool setup procedures to test the target network.	Setup should work properly.	8/23/2002	As expected
3	Execute the scan.	Scanning should proceed without errors.	8/23/2002	As expected
4	Compile and analyze the results. Detailed results will be included in a separate document. Summary statements of remaining vulnerabilities shall be contained in the Analysis of Results section.	All required security patches should be installed. No vulnerabilities impacting security requirements should be found.	8/23/2002	As expected

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(?) Analysis of Results:

(?) Pass/Fail:

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	

August 27, 2002

AUTOMATED VULNERABILITY SCANS AND RESULTS

(U) Test Case VS-01: Determine System Vulnerabilities Using the Internet Security Systems (ISS) System Scanner

(U) Description: This test runs the ISS System Scanner vulnerability assessment tool. The ISS System Scanner is a network-based security assessment and policy compliance solution. System Scanner provides ongoing and decision-support reporting focused on the most critical aspects of managing risk. The Internet Scanner can perform scheduled and selective probes of communication services, operating systems, key applications and routers. As it "scans," System Scanner uncovers the most comprehensive set of vulnerabilities likely to be exploited during attempts to breach or attack your network and provides you with the necessary corrective action. System Scanner also prepares reports and data sets to support sound, knowledge-based policy enforcement.

(U) Preparation: The Certification Test Team shall provide the ISS System Scanner with the latest vulnerability signatures. The System Administrator (SA) shall install the ISS Internet Scanner where needed.

~~(U)~~

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Install the Internet Security Systems System Scanner on server.	Test application should install properly.	8-22-02	As expected.
2	Execute the scanner tool setup procedures to test system server(s) for Internet Information Server vulnerabilities.	Setup should work properly.	8-22-02	As expected.
3	Execute the scanning as per setup.	Internet function scanning should proceed without a problem.	8-22-02	As expected.

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
4	Compile and analyze the results. Detailed results will be included as an attachment to this document. Summary statements of remaining vulnerabilities shall be contained in the analysis below.	A properly configured server should not exceed this number and/or severity of vulnerabilities. All required security patches should be installed.	8-22-02	As expected.

(U)Pass/Fail:

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>	<p>Pass</p>	
<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>	<p>Pass</p>	

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~F-37~~

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Test Case VS-03: Determine Windows Operating System Vulnerabilities Using the DISA Security Readiness Review Scripts

(U) Features of the DISA Security Readiness Review (SRR) Scripts: DISA Security Readiness Review (SRR) Scripts – These scripts are designed to check the access control of each system or database.

(U) Description: This test runs the DISA Security Readiness Review scripts. General features are described above.

(U) Preparation: The Certification Test Team shall provide the DISA SRR scripts. The system administrator (SA) shall install the DISA SRR script and batch files where needed.

(U) ~~(S)~~ Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Install the DISA SRR scripts and batch files on the network Primary Domain Controller.	Test scripts should install properly.	8/23/02	As expected. PDC is not setup for this configuration.
2	Execute the test scripts.	Server scanning should proceed without a problem.	8/23/02	As expected.
3	Compile and analyze the results. Detailed results will be included in a separate document. Summary statements of remaining vulnerabilities shall be contained in the analysis below.	A properly configured server should not have an excessive number and/or severity of vulnerabilities. All required security patches should be installed.	8/23/02	As expected.

(U) ~~(S)~~ Analysis of Results: It was noticed on both workstation and server that all auditing was not turned on. The system administrator said there was a resource issue when capturing all the auditing data. More details are included in the attached results.

(U) ~~(S)~~ Pass/Fail:

August 27, 2002

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	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(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.	Pass	
(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.	Pass	

August 27, 2002



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

WINDOWS 2000 SYSTEM POLICIES

(U) Test Case PS-W2K-01: Verify System Policies

(U) Description: This test identifies the elements of the Windows 2000 Security Policy as configured on the target system, and verifies compliance with requirements. Windows 2000 Security Policy elements are grouped into categories including Account Policies (lockout and password), Local Policies (audit, user rights, and security options), and IP Security. The Microsoft Management Console (MMC) is used to manage these security policy categories at the domain, group, user and local system levels.

(U) Preparation: The SA must be able to access the server. SA should provide, if available the preferred policy configuration settings for system servers and the basis for their use.

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~TOP SECRET~~

PG-44

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) Procedure:

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome
1	<p>From the MMC Console on the domain controller, observe the Default Domain Policy object. (On a workstation or member server, observe the Local Computer Policy object).</p> <p>Observe the objects located under Computer Configuration/Windows Settings/Security Settings.</p>			<p>Security Settings objects should include: <u>Account Policies</u> <u>Local Policies</u> <u>IP Security Policies</u></p> <p>(Additional Security Settings objects may include Event Log, Restricted Groups, System Services, Registry, File System, and Public Key Policies. At present, these additional objects are not managed via the MMC).</p>	As expected.
2	<p>Observe the Account Policies object, which should include the Password Policy and Account Lockout Policy objects. Open these two objects and verify that effective settings comply with requirements.</p>		<p>Password Policy</p>		

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
			Store password using reversible encryption for all users in the domain	Disabled	As expected
			Account Lockout Policy		
			Account lockout duration		
			Account lockout threshold		
			Reset account lockout counter after (time)		
3	Observe the Local Policies object, which should include the Audit Policy, User Rights Assignment, and Security Options objects. Open these three objects and verify that effective settings comply with requirements. Requirements notes: The following roles can be removed: Operators (Account, Backup, and Server), Guests, and Power Users.		Audit Policy		
			Audit account logon events	Success and Failure events audited	As expected.
			Audit account management	Success and Failure events audited	As expected.
			Audit directory service access	Success and Failure events audited	Not activated.
			Audit logon events	Success and Failure events audited	As expected.
			Audit object access	Success and Failure events audited	Not activated.
			Audit policy change	Success and Failure events audited	As expected.

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
			Audit privilege use	Success and Failure events audited	As expected
			Audit process tracking	Success and Failure events audited	As expected.
			Audit system events	Success and Failure events audited	As expected.
User Rights Assignment					
			Access this computer from the network	Administrators + (authorized groups)	As expected.
			Act as part of the operating system	Admin	Not assigned
			Add workstations to domain	Admin	N/A
			Backup files and directories	Admin Backup Operators	As expected
			Bypass traverse checking (prevents inheritance of permissions. Needed for IIS).	Admin (if IIS is hosted on this system, add Users)	Backup operators and Power Users also have access. Admin and everyone.
			Change system time	Admin	As expected
			Create pagefile	Admin	As expected
			Debug programs	Admin	As expected

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
			Deny access to this computer from the network	Admin	Not assigned on server.
			Generate security audits	Admin	Not assigned on server.
			Increase (disk) quotas	Admin	As expected
			Increase scheduling priority	Admin	As expected
			Load and unload device drivers	Admin	As expected
			Logon as a batch job	(as authorized and required)	As expected.
			Log on locally (from local console)	(Depending on application requirements, guests and anonymous users might be permitted for workgroup web servers on protected networks. However, if all users can be authenticated to the Domain Controller, then only Admins, Domain Users and required inter-server connections would be permitted.)	<p>The following group and users are allowed to logon locally:</p> <ul style="list-style-type: none"> Backup Operators Power Users Users Admin Guest
			Manage auditing and security log	Admin	As expected

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
			Restore files and directories	Admin	As expected
			Shut down the system	Admin	Backup Operator, Power Users, Users, Admin
			Take ownership of files and other objects	Admin	As expected
			Security Options		
			Additional restrictions for anonymous connections.	No	As expected
			Allow system to be shut down without having to log on	No	As expected
			Allowed to eject removable NTFS media	Admin	As expected
			Audit use of Backup and Restore privilege	Admin	As expected
			Automatically log off users when logon time expires (local)	No	As expected

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
			Clear virtual memory pagefile when system shuts down	Yes	As expected.
			Digitally sign client communication (when possible)	n/a	
			Digitally sign server communication (when possible)	n/a	
			Disable CTRL+ALT+DEL requirement for logon	No	As expected
			LAN Manager Authentication Level	Level 1 - Send LM & NTLM - use NTLMv2 (Kerberos) if negotiated.	n/a
			Message text for users attempting to log on	FBI Warning	As expected.
			Prevent users from installing printer drivers	Yes	As expected
			Prompt user to change password before expiration	Yes	As expected
			Rename administrator account	Yes	As expected

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
			Rename guest account	No. (Must be disabled)	Account disabled.
			Restrict CD-ROM access to locally logged-on user only	Yes	As expected
			Secure channel: Digitally encrypt secure channel data (when possible)	n/a	
			Unsigned driver installation behavior	No.	As expected
4	Observe the IP Security Policy object. Open the object, and verify that effective settings comply with requirements.		IP Security Policy		

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
			Client (Respond Only): Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.	Yes	No policy set for server or workstation.
			Secure Server (Require Security): For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients.	Not at this time	
			Server (Request Security) For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.	Not at this time	

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~F-50~~

PG-53

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) ~~(S)~~ Pass/Fail:

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.

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Requirement	Pass/Fail	Comment
(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.	Pass	
(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.	Pass	
(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.	Pass	

August 27, 2002

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: [Redacted]	Fail	
[Redacted]	Fail	
[Redacted]	Pass	
[Redacted]	Pass	
[Redacted]	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	

b2
b7E

August 27, 2002



System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

WINDOWS 2000 IDENTIFICATION AND AUTHENTICATION TEST SCRIPTS AND RESULTS

(U) Test Case IA-02: Test Password Requirement for System Access

(U) Description: This test confirms that the password belonging to that UserID is required for authentication and that any new password has to conform to requirements. It also checks that no password caching exists on the workstations examined.

(U) Preparation: System workstations shall be powered on, and logged in using the test user account created in the standard manner for the system, and made available to the testing staff. For Step 3, the system administrator must logon to one or more of each workstation type, as determined by baseline version.. Step 3 requires the examination of the local workstation registry. The system administrator should backup the registry if he/she is concerned about possible registry corruption during this test.

August 27, 2002

LIMITED OFFICIAL USE ONLY

~~F-54~~

PG-57

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

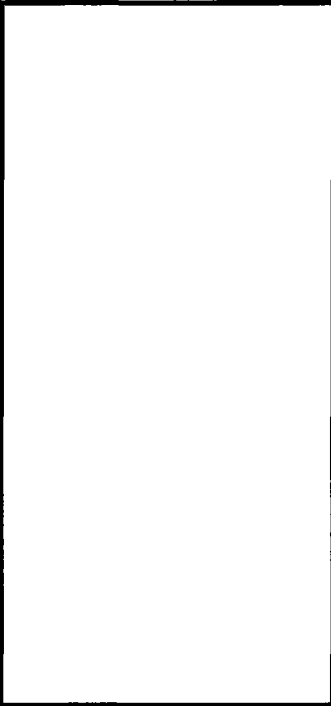
(U) ~~(S)~~ Procedure:

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
1	Testing staff shall logon to the test account, using the temporary password. Test person shall enter and confirm new password that satisfies requirements. Test person shall attempt to logon using misspelled passwords more than the maximum number of times allowed (4). Administrator shall reset password to default after login failure. Testing staff shall logon to the network using the new account and a new valid password. Repeat, entering a different valid password and confirm it.	User should be required to change password on first attempt after reset. Test person using new account created should be prompted to change password. Account should be locked if maximum number of attempts is exceeded. Logon after restoration should be successful. Attempting more than one successful change to a password in one day should fail. (Repeated changes to return to a favorite password should be discouraged.)	8/23/02	As expected

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
2	Using the test account, the testing staff person shall attempt to change the password, using several invalid examples. 	All cases (a) through (G) should fail. Using the initial password in New and Confirm Password fields should fail. Blank passwords, and passwords less than eight characters in length should fail. The system may or may not use a password filter (e.g., as in PASSFILT.DLL). If not, this is a finding. Valid new password should succeed.	8/23/02	As expected

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
3	<p>At each Windows NT workstation used in the previous steps, the SA shall log on as an Administrator. The SA will run the Registry Editor program (regedit or regedt32) and select the following key: HKEY_LOCAL_MACHINE\SOFTWARE.</p> <div style="border: 1px solid black; width: 200px; height: 150px; margin-top: 10px;"></div>	<p>Under no circumstances shall passwords be cached so to defeat their required use during system logon. However, local logon may be synchronized with the network logon that is controlled by an accredited server identification and authentication mechanism.</p> <p>The following should be found for Windows 9x and NT:</p> <div style="border: 1px solid black; width: 200px; height: 50px; margin-top: 10px;"></div> <p>The following value should be found for Windows 2000: 0</p>	8/23/02	As expected.

b2
b7E

(S) Analysis of Results: Password filtering was not turned on for the workstation or the server.

August 27, 2002

System Security Plan (SSP)

DCS 3000

Pre-Certification Test Results and Findings

(U) (S) Pass/Fail:

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: <div style="border: 1px solid black; height: 100px; width: 100%;"></div>	Fail	Password does not expire (e.g. DCSgod).

b2
b7E

August 27, 2002

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 05-19-2007 BY 85179DMH/KSR/LMF

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 record intercepted conversations into computer memory using digital technology. In addition to producing much higher quality and clearer recordings than the old tape technology, the use of this computer-based technology:

- Allows the field agent to easily and efficiently manage the recordings electronically *(Rather than having to sort, retrieve, and physically manipulate hundreds of tapes, an agent can find and listen to any previously recorded conversation with a few keystrokes on a computer.)*
- Facilitates the review and examination of the information
- Dramatically increases the efficiency of trial preparations
- Allows for the application of innovative techniques such as faster or slower playback, looping through selected portions of intercepts, and even the instantaneous playback of the beginning of a lengthy conversation while the conversation is still ongoing
- Supports the Field Translation Center concept, in that electronic (or digital) files of Criminal Law Enforcement (CLE) Title III intercepts can be transferred to a remote or distant field office for translation or transcription
- Exponentially increases the utility and value of computer-based intercepts

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

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

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

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

FOR OFFICIAL USE ONLY

2. RISK ASSESSMENT RESULTS

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

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

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

2.1. Risk Assessment

2.1.1. High Risk Vulnerability/Threat Pairs

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

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

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

Current Status:

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

2. There appears to be no password management in evidence. This practice will allow an unauthorized individual access to the system, compromising the system and any attached systems. Thereby, any evidence gained would be invalidated.

Current Status:

- Verified Closed

b2
b7E

FOR OFFICIAL USE ONLY

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

Current Status:

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

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

Current Status:

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

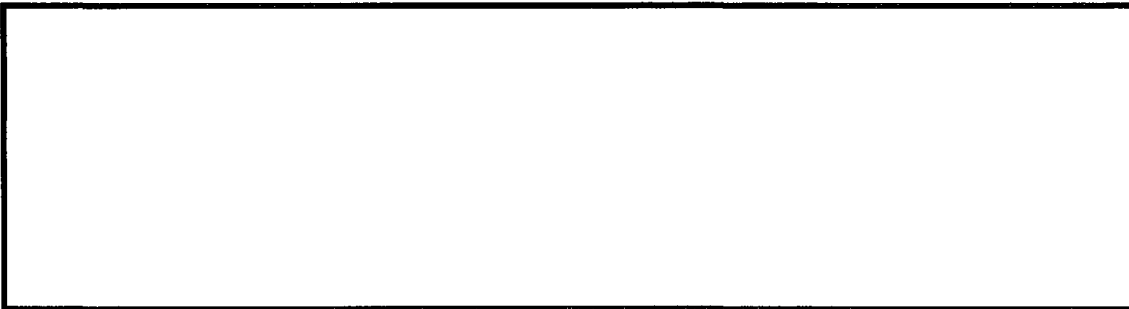
Planned or Recommended Remedial Action:

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

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

Current Status:

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



b2
b7E

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

Current Status:

- Verified Closed: Telnet is not being used.

2.1.2. Medium Risk Vulnerability/Threat Pairs

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

FOR OFFICIAL USE ONLY

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

Current Status:

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

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

FOR OFFICIAL USE ONLY

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

FOR OFFICIAL USE ONLY

RISK MANAGEMENT MATRIX FOR DCS-3000				
Risk Analysis			Risk Management	
Vulnerability (V)	Impact (I) or Asset	Significance (S) or Occurrence	Risk to Assets (R) or Likelihood	Mitigation or Recommended Control Measures (M) or Risk (RR)
5. Improper workstation permissions. VL = High	Workstations associated with the system do not enforce adequate user permissions. TL = Medium	Improperly configured machines do not adhere to the least privilege principle. SL = High	HIGH	Recommend the implementation of workstation permissions to give least privilege access. RR= Low
6. Improper guest/administrator account configuration. VL = High	Workstations allow guest accounts and have not deleted or renamed the administrator accounts. TL = High	The improper configurations do not provide the facility for adequate auditing. SL = High	HIGH	Closed
				b2 b7E
8. Telnet login is not encrypted VL = High	Telnet capability is unprotected. TL = High	Telnet login is accomplished in the clear. SL = High	HIGH	Closed

FOR OFFICIAL USE ONLY



DCS-3000

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-19-2007 BY 65179DMH/KSR/LMF

FOR OFFICIAL USE ONLY

1. INTRODUCTION

1.1. System Description

DCS3000 is a computer-based intelligence collection systems used by FBI personnel to record intercepted conversations into computer memory using digital technology. In addition to producing much higher quality and clearer recordings than the old tape technology, the use of this computer-based technology:

- Allows the field agent to easily and efficiently manage the recordings electronically *(Rather than having to sort, retrieve, and physically manipulate hundreds of tapes, an agent can find and listen to any previously recorded conversation with a few keystrokes on a computer.)*
- Facilitates the review and examination of the information
- Dramatically increases the efficiency of trial preparations
- Allows for the application of innovative techniques such as faster or slower playback, looping through selected portions of intercepts, and even the instantaneous playback of the beginning of a lengthy conversation while the conversation is still ongoing
- Supports the Field Translation Center concept, in that electronic (or digital) files of Criminal Law Enforcement (CLE) Title III intercepts can be transferred to a remote or distant field office for translation or transcription
- Exponentially increases the utility and value of computer-based intercepts

The DCS3000 system is deployed in central monitoring plants (CMP) located in FBI field offices and at the FBI Engineering Research Facility (ERF). Access to the field office buildings and the ERF is controlled by use of security guards, visitor badges, and visitor logs. Visitors are escorted at all times while in a field office building and at the

LIMITED OFFICIAL USE ONLY

ERF. Field office personnel monitor operations within the CMP, and operations are physically separated according to type and function (i.e., Title III versus Foreign Intelligence Surveillance Act [FISA] and computer operations versus case monitoring).

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

1.2. Risk Assessment Approach

The risk assessment for this system was conducted through:

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

2. RISK ASSESSMENT RESULTS

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

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

- 
- 
- 

b2
b7E

- Planned or recommended controls or alternative options for reducing risks

2.1. Risk Assessment

2.1.1. High Risk Vulnerability/Threat Pairs

The following are high-risk vulnerability/threat pairs that are drawn from the RMM table. There are seven operational aspects of this collection system that appear to be at high risk but easily mitigated. Overarching mitigating factors for these risks include the DCS3000 working environment at each operating location (i.e., FBI field office, resident agency (RA) office, etc.) that is tightly controlled and protected by multi-layered physical security, and the personnel within it, who participate in electronic surveillance (ELSUR)

LIMITED OFFICIAL USE ONLY

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

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

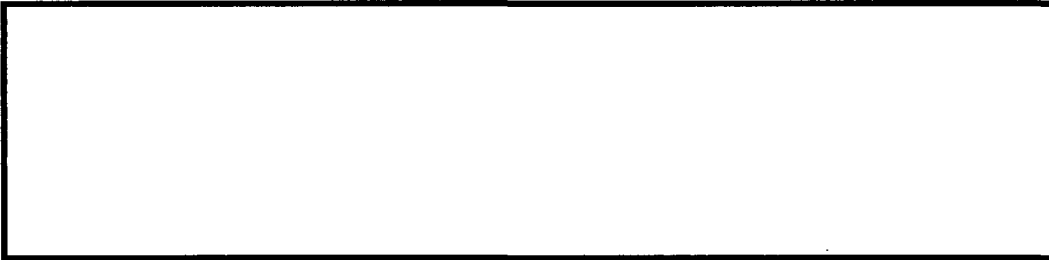
1. There is no anti-viral software loaded on the DCS3000 machines. If malicious code, viruses, and/or executables are introduced, there will be potential for risk to the system or compromise of data, thereby compromising evidence contained therein.

Planned or Recommended Remedial Action:

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

2. There appears to be no password management in evidence. This practice will allow an unauthorized individual access to the system, compromising the system and any attached systems. Thereby, any evidence gained would be invalidated.

Planned or Recommended Remedial Action:

- 
-
-
-

b2
b7E

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

Planned or Recommended Remedial Action:

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

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

Planned or Recommended Remedial Action:

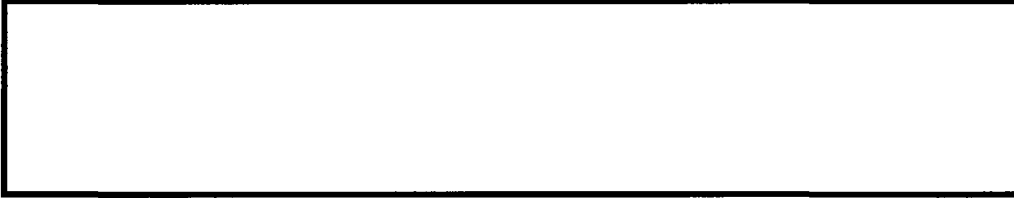
Recommend the implementation of workstation permissions to give least privilege access.

LIMITED OFFICIAL USE ONLY

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

Planned or Recommended Remedial Action:

Recommend deleting the guest accounts and renaming the administrator accounts.



b2
b7E

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

Planned or Recommended Remedial Action:

Recommend a secure Telnet implementation.

2.1.2. Medium Risk Vulnerability/Threat Pairs

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

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

Planned or Recommended Remedial Action:

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

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

RISK MANAGEMENT MATRIX FOR DCS3000				
Vulnerability (V)	Risk Analysis		Risk Assessment (R)	Risk Management (Mitigation or Recommended Control Measures, Residual Risk (RR))
	Threat (T) to A/C/F	Significance (S) of Consequences		
1. No anti-virus software found. VL = High	Introduction of malicious code, viruses and or executables to DCS3000 systems/networks without detection TL = High	If malicious code, viruses, and/or executables are introduced, there will be potential for risk to system or compromise of data SL = High	HIGH	Methods to be used to limit the risk: - Install FBI approved anti-virus software on all servers and workstations. - System administrators ensure all virus signatures are updated weekly or as needed. RR = Low
2. Insufficient password management controls VL = High	The system does not enforce adequate password policies, thereby allowing unauthorized access. TL = High	[Redacted] SL = High	HIGH	[Redacted] RR = Low
3. Insufficient account lockout policy VL = High	The system does not enforce an account lockout policy. TL = High	Without a lockout policy, an unauthorized user would have infinite attempts to gain access to the system. SL = High	HIGH	Recommend instituting an account lockout policy by implementing, at a minimum: - Account lockout duration - Account lockout threshold (i.e. 3 attempts) - Unlock procedures RR = Low
4. Inadequate audit logging. VL = Medium	Low gain from exploitation TL = Medium	Tracking users actions will allow records to be kept for accountability purposes. These records can be used for investigations and to track system or network problems for troubleshooting purposes. SL = High	MEDIUM	Recommend implementing workstation and server auditing and log dumps on a daily basis to reduce impact on resources. RR = Low

LIMITED OFFICIAL USE ONLY

RISK MANAGEMENT MATRIX FOR DCS3000				
Risk Analysis				Risk Management
Vulnerability (V)	Threat (T) or Asset	Significance (S) or Consequence	Risks to Assets (R)	Mitigation or Recommended Countermeasures (M) and Risk (RR)
5. Improper workstation permissions. VL = High	Workstations associated with the system do not enforce adequate user permissions. TL = Medium	Improperly configured machines do not adhere to the least privilege principle. SL = High	HIGH	Recommend the implementation of workstation permissions to give least privilege access. RR = Low
6. Improper guest/administrator account configuration. VL = High	Workstations allow guest accounts and have not deleted or renamed the administrator accounts. TL = High	The improper configurations do not provide the facility for adequate auditing. SL = High	HIGH	Recommend deleting the guest accounts and renaming the administrator accounts. RR = Low
[Redacted]				b2 b7E
8. Telnet login is not encrypted VL = High	Telnet capability is unprotected. TL = High	Telnet login is accomplished in the clear. SL = High	HIGH	Recommend a secure Telnet implementation. RR = Low

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/2/2006

To: Operational Technology

Attn:

[Redacted]

Security

Attn:

From: Security

Information Assurance/Accreditation/SPY-B F-501

Contact:

[Redacted]

Approved By:

[Redacted]

Drafted By:

: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.

b6
b7C

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

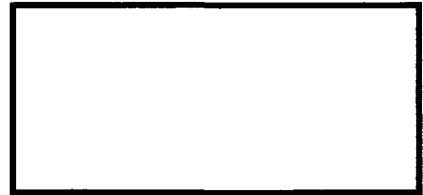
The DCS-3000 application suite was developed to assist Law Enforcement Agencies (LEA) with collecting and processing data for court-ordered Electronic Surveillance (ELSUR) operations. The DCS-3000 collects J-STD-25 data from the Telecommunications Service Provider (TSP) and stores it at the LEA site.

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.

b6

The Certification and Accreditation Team Members are: b7C

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



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

◆◆

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# 92

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 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.

Sincerely,

William L. Hooton
Executive Assistant Director

Enclosure

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-25-2007 BY 65179/DMH/KSR/LMF



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

May 28, 2003

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

b6
b7C

Dear Mr. [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,

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-25-2007 BY 65179/DNH/KSR/LMF

William L. Hooton
Executive Assistant Director

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

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/19/2002

To: Director's Office
Information Resources

Attn: Mr. [redacted] Room 7128
Mr. [redacted] Room 4272
Ms. [redacted] Room 4282

From: Director's Office
Security Division, Information Assurance Section (IAS),
Room 9396

Contact: [redacted] 202-[redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] js

Case ID #: 66F-HQ-C1333650-DCS3000 (Pending)

Title: SYSTEM CERTIFICATION AND ACCREDITATION
Data Collection System (DCS) 3000

Synopsis: This EC documents the security certification and recommends the type accreditation of the DCS3000. In accordance with the provisions of OMB Circular A-130 and in general conformance with NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), guidance, the DCS3000 is hereby certified as providing the safeguards and security features required for secure operations.

Details: The DCS3000 system is certified to operate at the sensitive-but-unclassified (SBU) level and the system-high mode of operation. All users have formal access and need to know for all information on the system.

The IAS Test Team conducted a comprehensive pre-certification system vulnerability assessment (P-SVA) of this system. The favorable results of the P-SVA eliminated the need for any further follow-on testing of this system. However, an action plan was developed to address the P-SVA findings/system vulnerabilities documented in the assessment and has been included in Section 5 of the enclosed DCS3000 System Security Plan. The action plan shows that corrective actions for all findings have been accomplished, and that all findings have been closed with associated risks mitigated as of December 16, 2002.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-25-2007 BY 65179/DMH/LSR/LMF

To: Security From: Director's Office
Re: 66F-HQ-C1333650-DCS3000, 12/17/2002

Recommend the DCS3000 system be type accredited for continued operation.

To: Security From: Director's Office
Re: 66F-HQ-C1333650-DCS3000, 12/17/2002

LEAD(s) :

Set Lead 1:

SECURITY

AT WASHINGTON, DC

The Accreditation Unit in the Security Division should review the DCS3000 documentation and determine the accreditation status.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

For information only.

CC: 1 - Mr. [redacted] Room 9396
1 - Ms. [redacted] Room 9483
1 - [redacted] FBI Engineering Research Facility
1 - [redacted] FBI Engineering Research Facility

b6
b7C

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:

mgm

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

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).

Reference: 66F-HQ-C1333650-DCS3000

Details: The Data Collection System 3000 (DCS3000) is certified to operate at the SBU level, Dedicated mode of operation. It is a Tier 1, Protection Level 1 system with Confidentiality - Medium, Integrity - Medium and Availability - Medium.

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 Windows 2000 platform. Although the system is connected only to a Telephone Service Provider for passive monitoring, data is transferred daily, via removable media, to the Telephone Application (TA) on FBINet. 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.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-25-2007 BY 65179/DMH/KSR/LMF

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).

◆◆

LIMITED OFFICIAL USE ONLY



DCS3000
System Rules of Behavior
APPENDIX D

March 13, 2003

b6
b7C

Prepared For:

Ms.

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

Prepared By:

The LSCU Green Team
FBIHQ

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:

- Your unique personal identifier (user ID) on the system; Your user ID will be used to control your access to parts of the system and for auditing your activities on the system

LIMITED OFFICIAL USE ONLY

- Your password on the system; the system will ask for your password to authenticate your identity, before granting you access. You may get a temporary password; if you do, the system will ask you for a new one the first time you log on. You should also be notified of any requirements for password length, content, duration, etc. Never write your password down.
- Your access privileges; your access privileges may be limited to a specific list of file areas, programs, and activities.

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

Contact:	Description of Duties:	Telephone:
Project Manager [Redacted]	Project manager for DCS3000 activities.	
Information Systems Security Officer (ISSO) [Redacted]	Ensures that the information system is implemented with appropriate security features and meets the minimum security requirements.	
DCS3000 Senior System Technical Representative [Redacted]	Serves as senior technical advisor for all DCS3000 issues	
Switch-Based Intercept Program Manager [Redacted]	Serves as POC for all DCS3000 switch-based intercept issues	
User Representative [Redacted]	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.	TBD

b6
b7C

Table 1: Contacts

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:

- Degauss the media (erase all magnetic patterns)
- Destroy the magnetic medium physically (e.g., open the plastic floppy disk casing, remove the disk, and shred it)
- Use an approved software program to completely delete all files on the medium and overwrite them with ones and zeroes

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

Passwords

The following password management policy is taken from the DOJ 2640.2D or the FBI MIOG.

- Do not record your password in writing.
- Do not share your password or accept another user's password if offered. Sharing passwords defeats the system's user identification and authentication mechanisms. In addition to sharing access privileges, participants share liability for any unauthorized behavior traced to the shared UserID and password.

LIMITED OFFICIAL USE ONLY

- [REDACTED]
- Your password should be something you can easily remember.
- Passwords should not be something that another individual can guess. Therefore, do not use the name of your spouse, pet(s), or children. Passwords that contain a word(s) is (are) susceptible to being guessed by software routines that check every word in the dictionary.
- [REDACTED]
- System administrators have no way to look up your password. If you forget it, your system administrator will have to change it and make you pick a new password.
- The system will prompt you to change your password every 90 days.
- A new password cannot be one you used recently. The system will not allow the use of any of the last six passwords used.
- If there is a reason, you may change your password before the end of 90 days.
- Users will be locked out of the system after four consecutive incorrect password entries and will be required to contact the system administrator.
- [REDACTED]
- A user's screen saver password should have the same characteristics as the password used to log-on to DCS3000, but will be different from the system password.

b2
b7E

1.2 Interacting With Administrators

Occasionally, users need to call upon administrators at various levels in order to obtain services or meet requirements for the task at hand. Some routine occasions are listed below.

- When you start a new job, or your job description changes, coordinate your DCS3000 access requirements and parameters with your supervisor.
- When you need to obtain membership in a shared directory, or change or terminate your membership privileges, see your supervisor and the owner of that directory.
- When you need other access privileges in order to do your job, notify your supervisor.

LIMITED OFFICIAL USE ONLY

- When you find that your access to DCS3000 resources is beyond what you need to do your job, notify your supervisor.
- In the event of a DCS3000 system crash during the absence of the system administrator, users will look in the office safe for instructions, UserID and Password for the alternate system administrator account and reboot the system.

When you need to remove any computer resource from DCS3000 premises, see your supervisor for approval; follow FBI regulations when removing any devices from the premise. Resources may only be removed from DCS3000 premises for official use.

1.3 Configuration Management

Configuration management addresses changes to DCS3000. It is important to understand that changes, (minor or major) to the system can greatly effect it's security posture. Changes must be identified, reviewed, and possibly evaluated prior to incorporating them into the system. The Configuration Management Board, along with the Information Assurance section within the Bureau, will review and decide if the changes require re-certification of the system.

1.3.1 Things You May Change

You may share directories and files, provided you limit the number of people who can access your files.

If you do share directories or files, you may change the list of users with access, as needed. You should review this list, at least quarterly, to ensure it is limited to people who need access.

You may change the Windows "wallpaper" background on your workstations and or servers. The only requirement is that of good taste.

1.3.2 Things You May Not Change

Do not install any software onto your workstation or any other DCS3000 resources. Only the DCS3000 system administrator (or his/her designated representative) is authorized to load software on workstations or servers. This must be coordinated with DCS3000 Program Manager

Do not attempt to add printers of any kind. If you need access to another printer, see your supervisor or system administrator. Normally, users will be assigned to the printer nearest to their workstation area.

Do not add any additional hardware or peripheral devices to any workstation, server or other DCS3000 resource. This includes all devices such as extra memory, hard drives, printers, scanners, additional servers, additional processors, etc. These tasks are handled by the system administrator and subject to configuration control.

LIMITED OFFICIAL USE ONLY

1.4 Unauthorized Activities

All DCS3000 users are held strictly accountable for their actions while on the system. User activity may be monitored and system activity audited to detect unauthorized behavior. Unauthorized activity may result in a warning, reprimand, loss of access, formal disciplinary action (including dismissal), or even legal action (such as a fine or imprisonment).

Unauthorized activities include:

- Entering unauthorized, inaccurate, or false information. Do not delete or manipulate information inappropriately.
- Using data for which you have not been granted authorization. Do not explore data or IS capabilities that are not related to your job or attempt to access information which you do not have authority to access. If you have any questions about the limits of your authorization, consult your supervisor for clarification.
- Retrieving information for someone who does not have access to it himself/herself, except as specifically authorized in your job description, or by your supervisor.
- Violating copyright and site licenses of proprietary software. This may happen when multiple copies of licensed software is installed, as well as when unlicensed software is installed.
- Installing unauthorized software. Do not install outside software (including other agency software, shareware, freeware, personally purchased, or pirated software) on DCS3000.
- Installing modems (either internal or external) on a workstation, server or any other DCS3000 resource. Although covered in the preceding section on configuration management, modems deserve special attention because they are a well-known way to bypass firewall protection or give remote access to unauthorized individuals. In particular, modems that are set to answer calls enable system access from outside the facility and may be regarded as a malicious breach of security.
- Storing or processing classified national security information on DCS3000. If, for any reason, classified information is introduced to DCS3000, notify your system administrator as soon as possible.
- Leaving your computer logged into the system when not being used. Log-off your workstation whenever you are away from the immediate work area, unless the Windows screen saver feature with a password enabled is properly invoked.

LIMITED OFFICIAL USE ONLY

1.5 *Your Role in Protecting the System*

Ensure that any data that is visible on the workstation monitor screen cannot be viewed by unauthorized personnel. The following guidelines will be followed when using the Windows NT/2000 screen saver option:

- Only the Windows screen savers are authorized. No other screen savers shall be installed.
- The password option for the screen saver will be invoked by the user. The password created will be generated by the user. The criteria for generating that password will be the same as that used for creating a DCS3000 log-on password.
- The screen saver password and DCS3000 log-on password will not be the same nor should one be a derivative of the other [redacted]. This makes it much easier for an individual to guess your password.
- The user will ensure that the screen saver activates before leaving the workstation unattended. This must be done, because there are conditions in a session that will delay or preclude the screen saver from activating (e.g., the print pop-up is present on the screen, data exchanges are occurring between Server and workstations, etc.).

b2
b7E

Ensure printouts are retrieved as soon as possible. Output should not be left unattended for any longer than is necessary.

Protect your equipment (workstation, diskettes, etc.) from physical damage. Ensure that your workstation is clean, ventilated, and located in a place where it is not likely to be bumped or knocked over. Keep food and drinks where they won't get spilled on the equipment.

Safeguard DCS3000 resources against waste, loss, abuse, unauthorized use, and misappropriation.

Scan all disks for viruses before use, especially if they are received from external sources. Discontinue use of any DCS3000 resources that show indications of being infected by a virus and immediately report any incidents to the ISSO.

Report any security incidents or suspected security incidents, including computer virus infections, to your ISSO. The term "security incident" includes any event that may result in the disclosure of sensitive information to unauthorized individuals or that results in unauthorized access, modification or destruction of system data, loss of system processing capability, or loss or theft of any computer system media.

Challenge any unauthorized personnel in your work area.

To meet minimal accreditation standards, all FO DCS3000 must have a Rules of Behavior in place. It is paramount that the ISSO, System Administrator, and all users read and follow these Rules of Behavior. A generic accountability sheet is shown in the back of this document.

LIMITED OFFICIAL USE ONLY

2.0 USER SUPERVISORS

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

2.1 *Account Creation Responsibilities*

First line supervisors are responsible for requesting access to DCS3000 for new users and the granting of new access privileges that may be required by users under his/her supervision.

2.2 *Account Termination Responsibilities*

First line supervisors are responsible for directing the removal of DCS3000 access for all persons under their supervision upon transfer of the user, termination of service or when there is no longer any need for that user to access DCS3000 resources. The supervisors should:

- Notify the ISSO and system administrator upon the departure or transfer of all assigned staff (government employees, contractors, etc.).
- Ensure continued availability of information when an employee terminates. Transfer employee files to another authorized user when needed, delete unnecessary files, and get passwords to encrypted files.
- Counsel terminating employees on nondisclosure of sensitive information.
- Terminate access to information and computer systems immediately in the event of unfriendly separation. Physically remove an employee when there is likelihood of sabotage.

2.3 *Account Parameters*

First line supervisors may request the establishment of shared directories. When a shared directory is established, the following rules apply.

- The first line supervisor is responsible for designating those users who will be granted access to such directories and the permissions to be assigned to each user.
- An owner will be assigned to manage each shared directory.
- The first line supervisor is responsible for ensuring that owners review and verify the list of authorized users for each shared directory at least quarterly. The shared directory owner will request termination of access for any user no longer requiring access.

2.4 *Account Verification/Validation*

Supervisors will respond to system administrators' annual requests for review of user privileges.

2.5 *Awareness Responsibilities*

Supervisors will ensure that all DCS3000 users belonging to, or performing work within, their

LIMITED OFFICIAL USE ONLY

organization have current knowledge of these Rules of Behavior, the required clearance, and a need-to-know for all information they are authorized to access.

2.6 Official Use

Supervisors will ensure that the system is not used for any unlawful, immoral or unethical activities.

2.7 Incident Reporting

Supervisors are responsible for ensuring that security incidents are promptly reported to the ISSO.

3.0 ADMINISTRATORS

These Rules of Behavior apply to all Administrators for DCS3000.

3.1 System Administrators

3.1.1 Responsibilities

In addition to compliance with the Rules of Behavior that apply to all users, DCS3000 system administrators are responsible for:

- Verifying the adequacy and authenticity of a new user's request before authorizing the creation of his/her new user account. Contact ISSO for any specific security questions when creating an account.
- Ensuring software has been approved by the Configuration Control Board (CCB) and Information Assurance section before installing.
- Becoming thoroughly familiar with and complying in all respects with the requirements of DCS3000 Security Policy and these Rules of Behavior.

LIMITED OFFICIAL USE ONLY

- Supporting and providing technical assistance to supervisors and the ISSO in the performance of their duties and responsibilities relating to the security of DCS3000.
- Managing the creation and deletion of user accounts and the granting and revocation of system privileges.
- Maintaining and keeping current all system documentation
- Altering the configuration of DCS3000 hardware or software only in accordance with the requirements of the Configuration Control Board.
- Initiating an annual review of any advanced access privileges they have granted, to verify that personnel still need access. System administrators will generate lists of personnel who have advanced privileges and send them to the appropriate supervisors for review and written response. If a supervisor determines that some personnel no longer need advanced privileges, the system administrator will terminate their access.
- The system administrator will rename the primary system administrator account and use it to create additional system administrator accounts with full system administrator privileges. The UserID for these accounts can be any valid logon name (i.e. DCS_ADMIN), but cannot be SYS_ADMIN. The user ID and password for the primary system administrator account (together with instructions) will be kept in a marked envelope in an office safe. DCS3000 users are instructed to look in the safe for system administrator instructions, UserID and password in the event that the DCS3000 system needs to be rebooted.

3.1.2 Separation of Duties

System administrators will use their system administrator user ID and privileges only when performing system administration duties. They will use a general user ID and privileges for all other duties. Duties that entail security of the IT system shall be separate from administrator duties and assigned to two different personnel, when possible.

3.2 ISSO

The ISSO is responsible for:

- Maintaining a document library containing current copies of all security plans, policies, regulations, certification and accreditation documentation, and procedures applicable to DCS3000.
- Becoming thoroughly familiar with the DCS3000 security plan, DOJ 2640.2d policy, FBI MIOG requirements and basic best practice security procedures and standard operating procedures..
- Ensuring the implementation of the DCS3000 Security Plan and its development, operation and maintenance in accordance with the requirements of the DCS3000 Security Policy and all other applicable security policies, regulations and procedures.

LIMITED OFFICIAL USE ONLY

- Monitoring the administration of DCS3000, providing guidance to system administrators and ensuring their compliance with all such security plans, policies, regulations and procedures.
- Ensuring that physical access control procedures and measures are properly implemented at the sites for which they are responsible.
- Implementing and ensuring compliance with the requirements of the security incident reporting program.
- Providing advice and assistance to managers and supervisors in performing their duties in relation to the DCS3000 security program.
- Assisting site managers in the selection and use of safeguards that reduce the risk to systems and facilities from malicious software and intrusions.
- Assuring that system security plans are revised and assisting in the re-certification and accreditation of the system according to the requirements of the DCS3000 Security Plan.

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

The following warning notices will be used as indicated to inform users of FBI information systems that such use is subject to information systems security monitoring.

LIMITED OFFICIAL USE ONLY

5.1 Computer Log-on Banner

***** WARNING *****

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, activities on this system are monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

***** WARNING *****

Do you accept these requirements and conditions? (Y/N)

6.0 SYSTEM ADMINISTRATORS

6.1 Objective

The two main goals of the system administrator (SA) are to keep the AIS (automated information system) operational and secure. The following tasks are essential in accomplishing these goals:

- Ensure that the operating system for the AIS is configured properly and that the security features appropriate to the intended level of system operation are properly set. Such settings should be periodically reviewed; such reviews will not involve looking at information or data contained in the files of individual users other than system configuration files.
- Use approved tools to periodically review system security. These may be security utilities provided with network software. At no time will the utilities be used to review user data even if the tool is capable of this function.
- Periodically check with the operating system manufacturer in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate in order to maintain AIS security.
- Ensure audit software is properly configured and audit trail reports are periodically reviewed in accordance with this document.

Review file names, length, permissions, and directories. If any of this information leads a SA to suspect that an individual user is misusing the system or engaging in other misconduct, the SA will notify the ISSO. The ISSO will contact the Special Agent in-Charge (SAC) for that field office. The SAC will contact Criminal Investigation Division (CID). At no time will the SA specifically target or track an individual's activities except as part of a properly authorized investigation.

i

LIMITED OFFICIAL USE ONLY

LIMITED OFFICIAL USE ONLY

If a SA suspects an unauthorized user is attempting to access the AIS, the SA is authorized to take the actions necessary to verify and limit the penetration attempt from an unauthorized user. Once verified, the SA will notify the ISSO. The SAC will contact CID. The SA may make system backups of appropriate log, history files, and user directories. Once the SA has determined that the anomaly is in fact an unauthorized intrusion, and CID have been notified, the SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation.

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

The SA does not have unlimited authority in operating the AIS. While security of the system is an important component of the administrator's job, there are restrictions on actions that an administrator may take in accomplishing the security function:

The SA is NOT authorized to view, modify, delete, or copy data files that are stored on the AIS which are not part of the operating system except when:

- Authorized by the user or file owner.
- Performing system backup and disaster recovery responsibilities.
- Performing antivirus functions and procedures.
- Performing actions which are necessary to ensure the continued operation and system integrity of the AIS.
- Performing actions as part of a properly authorized investigation.

The SA is NOT authorized to browse or read a user's E-mail. The SA may intercept, retrieve, or otherwise recover an E-mail message upon the written or verbal authorization of the parties involved or as part of a properly authorized investigation. When the SA must remove an E-mail message that is interfering with the operation of the AIS, the SA will make reasonable effort to notify the originator of the E-mail.

The SA is NOT authorized to use hacker techniques in an attempt to penetrate his or her AIS. Techniques include but are not limited to:

- The use of network analyzers, sniffers, or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized to perform valid system troubleshooting and diagnostics of network problems.
- "Keystroke monitoring" software of any kind will not be used either resident on the user's computer, or by monitoring computer network communications.
- The use of keyboarding or automated techniques to exploit/verify vulnerabilities identified by the C2 Protect tools.

LIMITED OFFICIAL USE ONLY

6.3 Management Searches

In the absence of a user, the SA is authorized to grant the user's supervisor temporary access to the user's data files, in order to allow access to data for official purposes. When such access is granted:

The SA will brief the supervisor as to the limits of accessing the user's data files. This will include a warning that the search must be limited in scope to those files that could reasonably be related to the objective of the search (that is, E-mail access would NOT be reasonable when searching for a word processing file). Searches will be limited to the time necessary to locate the required data.

Such access will not be used to circumvent regulatory or statutory requirements for investigations.

6.4 Assistance to Law Enforcement and Counterintelligence

The SA is authorized to provide technical assistance as requested by the investigating agent when part of a properly authorized investigation.

LIMITED OFFICIAL USE ONLY

DCS3000/Privileged User Rules of Behavior Acknowledgement Form

As the privileged or super user of the DCS3000 Automated Information System (AIS), I acknowledge my responsibility to conform to the following requirements and conditions as directed by Department of Justice Order (DOJ) 2640.2D (Information Technology Security), DOJ-TS-001 (DOJ Access Control Standards Password Management), Manual of Investigative Operations Guidelines Part 2, Section 26 (Classified National Security Information and Material) & 35 (FBI Automated Data Processing and Telecommunications Security Policy), the SACS System Security Authorization Agreement, and local Security Operating Procedures (SOP). DCS3000 is an FBI-accredited network. These conditions are established for and apply to all AIS connected to DCS3000.

1. I understand that failure to sign this acknowledgment will result in denial of access to DCS3000.
2. I understand the need to protect the "root" or "super user" password at the highest level of data it secures. I will not share the root or super user password and/or account with any unauthorized persons.
3. I understand I am responsible for all super user or root actions taken under my account. I will not attempt to "hack" the network or any connected AIS, or any connected network. I will not attempt to gain access to data for which I am not specifically authorized, to include E-Mail and users files in their home directories. I will only use my special accesses or privileges to perform authorized tasks or mission-related functions on DCS3000.
4. I understand my responsibility to report any/all IS or network computer security problems to the: Information System Security Officer (ISSO) and the Security Countermeasures Program Manager (SCMPM).
5. I acknowledge my responsibility to use the network only for official government business. I understand I am required to report the discovery of any violations of this rule to the DCS3000 ISSO.
6. I will not enroll any user to the network or any connected system that is not approved by their supervisor (or sponsor in the case of non-FBI employees) and cleared to at least the TOP SECRET level.
7. I understand that the network operates in the Sensitive But Unclassified condition/level. I have all clearances necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by DCS3000 System Security Policy.
8. I understand my responsibility to appropriately protect all output generated under my account, to include printed output, magnetic tapes, floppy disks, and downloaded hard disk files. I understand that I am required to ensure all hard copy output and magnetic media is properly labeled as required by the regulations listed above.

LIMITED OFFICIAL USE ONLY

9. I understand my responsibility to not introduce any software or hardware not acquired through official channels. I also acknowledge my responsibility to virus-scan all official and authorized software before introducing it into DCS3000.

10. I acknowledge that all DCS3000 equipment and related items are for the communication, transmission, processing, and storage of U.S. Government information only. These systems and equipment are subject to monitoring to ensure proper functioning, to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features and procedures, and for like purposes. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by any user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. In using this system, I expressly consent to such monitoring.

11. I will not violate any U.S. statute, and I understand that I am bound by the directives of the President of the United States, the Attorney General, Director of Central Intelligence (DCI), the Director FBI, Rules of Behavior, and local Standard Operating Procedures (SOP). I further understand that I cannot be ordered by any lesser authority to violate either the letter or the spirit of any U.S. statute, Executive Order, directive from the A6 DOJ, DCI, Director FBI, or local SOP. I bear sole responsibility and liability for any such violation. Suggested reading for this includes the Privacy Act of 1974, National Computer Security Act of 1987, Executive Order 12958 (Classified National Security Information), Department of Justice Order 2640.2D (Information Technology Security), DOJ-TS-001 (DOJ Access Control Standards Password Management), and Manual of Investigative Operations Guidelines Part 2, Section 26 (Classified National Security Information and Material) & 35 (FBI Automated Data Processing and Telecommunications Security Policy).

12. I acknowledge my responsibility to conform to these requirements and conditions when using DCS3000 Network/Systems. I also acknowledge that failure to comply with these requirements and conditions may constitute a security violation resulting in denial of access to DCS3000 Network/Systems. Additionally, such violations will be reported to the appropriate authorities for further action as deemed appropriate.

13. I have completed the required course(s) and secure awareness training prior to receiving access to DCS3000.

14. A copy of this agreement will be kept on file with the DCS3000 ISSO as part of my security agreement.

Privileged User Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

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

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

b6
b7C

Prepared By:
LSCU Green Team
FBIHQ

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-05-2007 BY 65179DMH/KSR/LMF

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 Personnel3
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 Recovery.....8
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

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

The DCS3000 was developed by personnel from the Telecommunications Intercept and Collection Technology Unit (TICTU) of the Cyber Technology Section of the Federal Bureau of Investigation (FBI). The TICTU is located at the FBI Engineering Research Facility (ERF), Building # 27958A, Quantico, VA 22135.

The DCS3000 has been in operation since 1997 and is operational in 55 of 56 FBI field offices across the United States.

1.4. Assumptions

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

- The clearance process is adequate to reduce the risk of insider threat.
- Adequate physical access controls are being implemented as planned.
- Interconnected network elements outside the scope of this system are secured.

2. REFERENCES

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

- FBI Certification and Accreditation Handbook (Draft), October 17, 2002
- FBI, *Manual of Investigative Operations and Guidelines* (MIOG), Part II, Section 35
- FBI, *Manual of Administrative Operations and Procedures* (MAOP) Part I, Section 259, *Security Clearance Investigations*

3. CURRENT OPERATING ENVIRONMENT

3.1. Current System

To conduct court-ordered ELSUR operations, LEAs dial into switches that are devices used by telecommunications service providers to route telephone calls to their destinations. The DCS3000 can collect ELSUR data under the following warrant types:

- **Pen Register** - limited to call data
- **Title III** - limited to call data and call content
- **Cooperative Warrant** - limited to call data and call content for phone numbers that do not belong to identified associates.

3.2. Major System Components

The DCS3000 suite consists of five 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 DCS3000 consists of the following applications:

- Client
- Server
- MultiServer
- VANGuard
- MultiVANGuard

The Client

The client is used to enter warrants, and to collect incoming call data and record call content in formats that are appropriate for use as evidence. Surveillance operations can be interrupted or closed from the client. The client is required for surveillance operations unless these capabilities are performed via a third-party application such as a collection platform.

The client may collect data within the following guidelines:

- Support one Title III, Cooperative Warrant, or one Push-to-Talk (PTT) collection and /or
- Support multiple Pen Register collections
- Connect to multiple servers or MultiServers (up to 35)

The Server

The server receives data from the switch and routes that data to the client. The server is the only application that can receive and route data for PTT calls. The server can support the following:

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

The MultiServer

The MultiServer provides the same functionality as the server, except that it has the ability to connect to multiple switches. It is sometimes referred to as the Multiple Switch Server. In addition to multiple-switch connections, the MultiServer can support the following:

- Multiple Title III and Cooperative Warrant collections
- Support multiple Pen Register collections
- Multiple client connections

The VANGuard

The VANGuard buffers data from [redacted]-compliant [redacted] switches, and routes the [redacted] data to the server or MultiServer. It enables field offices to collect data periodically, thus saving on potential long distance charges. While multiple switches can connect to the VanGuard, the VanGuard can connect to only one switch.

The Multi-VANGuard

The Multi-VANGuard can buffer data from multiple [redacted] switches. It can be referred to as the Multiple-Switch VANGuard. Like the VANGuard, the Multi-VANGuard enables field offices to collect data periodically, thus saving on potential long distance charges. This application can, also, be used to monitor the status of current connections. Users can reset a connection if a problem is detected. The VanGuard can connect to up to 25 switches.

b2
b7E

3.3. User Organizations and Personnel

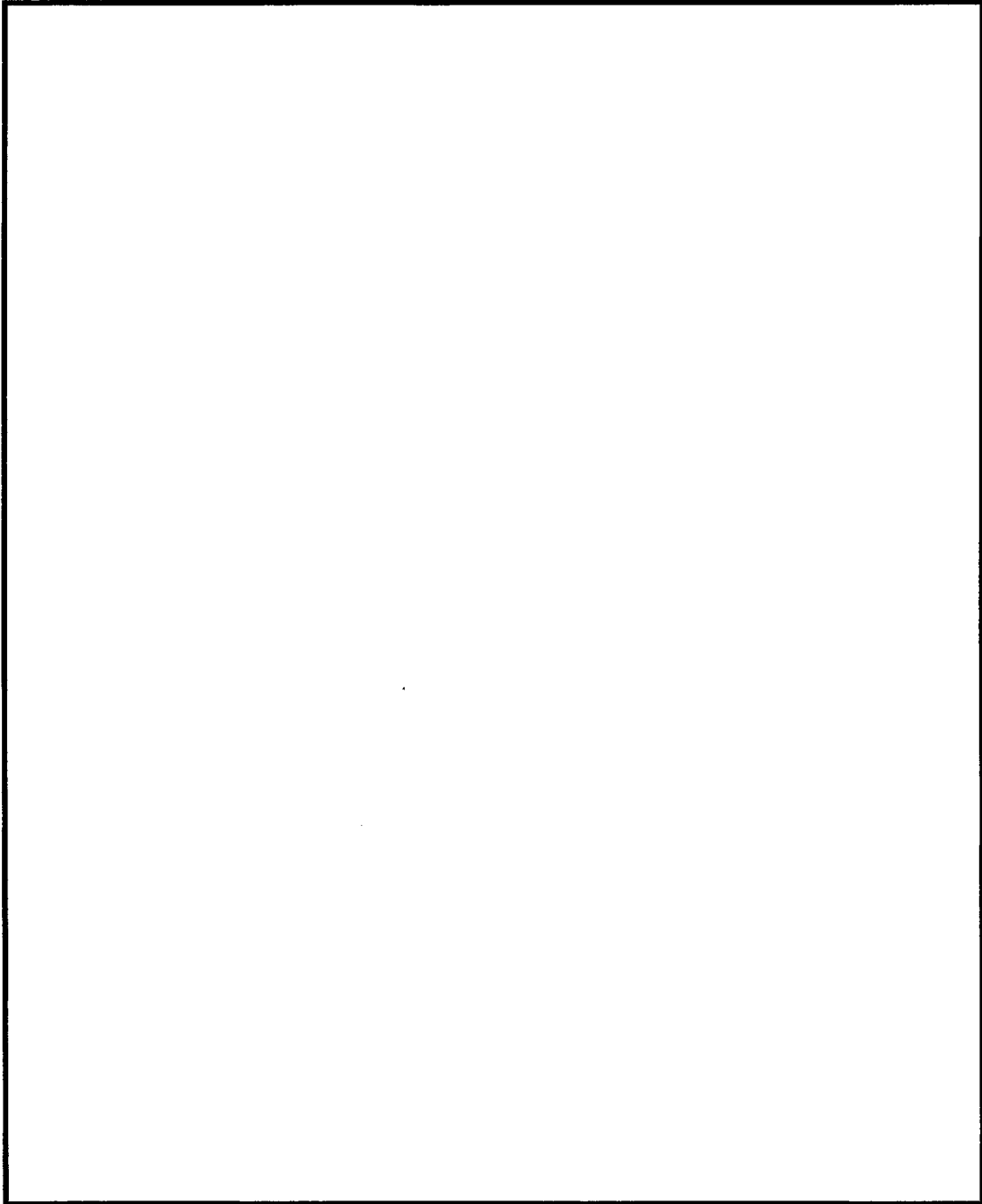
In addition to cognizant system management and engineering personnel at the TICTU located within the FBI ERF, other user personnel are found at FBI field offices throughout the United States and Puerto Rico.

4. SYSTEM OPERATIONAL OVERVIEW

4.1. Networking Infrastructure

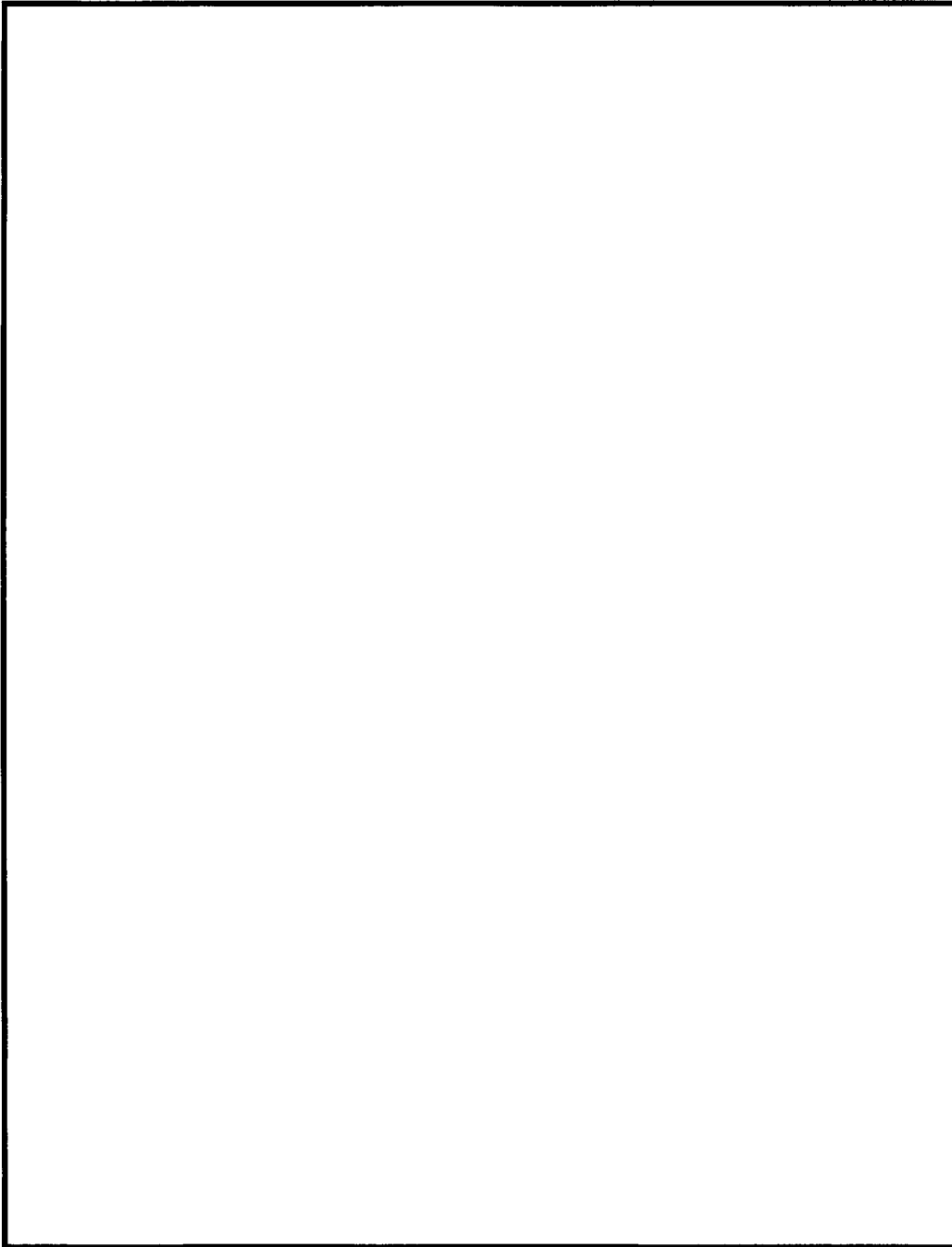
The DCS3000 is connected to the telecommunications service provider via TCP/IP. The connection can be established either by the DCS3000 or by the switch. Data transmitted to the DCS3000 in support of Title III, Pen Register, or Cooperative Warrant collections is sensitive-but-unclassified (SBU).

The DCS3000 is a modular system that can be set up and configured to meet specific case needs. Figure 1 represents a typical configuration for Pen Register collections. Call data is provided from the switch to the VanGuard, which stores the data temporarily, until it is collected by Multiserver and forwarded to the client. The Multiserver and client could reside on the same workstation. Figure 2 represents a typical configuration for Title III collections at one LEA location. In this case the Multiserver and clients are connected via a LAN. Call content is provided on a channel independent of the call data.



b2
b7E

Figure 1. Typical DCS3000 Configuration – Pen Register



b2
b7E

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
	TCP/IP over ISDN	Dial-out from switch to directory number
	TCP/IP over leased line	Dial-out from switch to directory number
	TCP/IP over dedicated connection (frame relay or VPN)	Dial-out from switch to directory number
	TCP/IP over dedicated connection	Dial-out from switch to directory number
	TCP/IP over X.25, ISDN BRI	T1

b2
b7E

4.2. Information Transfer and Collaboration

The DCS3000 is connected to and transfers data from the telecommunications service provider via TCP/IP. The connection can be established either by the DCS3000 or by the switch.

4.3. Hardware

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

4.3.1. Workstations

DCS3000 can be installed on any Pentium-based workstation running Microsoft Windows 2000. The minimum memory requirements are the same as the minimum required for running the operating system.

Client workstations must have a Recorder Control Interface (RCI) card and recorder to support a Title III collection. A separate Client workstation is needed for each Title III target.

4.3.2. Data Communications Equipment

DCS3000 uses the following telecommunications equipment to establish data communications:

- Cisco 1610 router
- US Robotics Courier V.Everything External Modem

4.4. Software

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

4.4.1. Operating System

All DCS3000 applications run under the Microsoft Windows 2000 operating system.

4.4.2. DCS Applications

Please refer to section 3.1 above.

4.4.3. Security Software

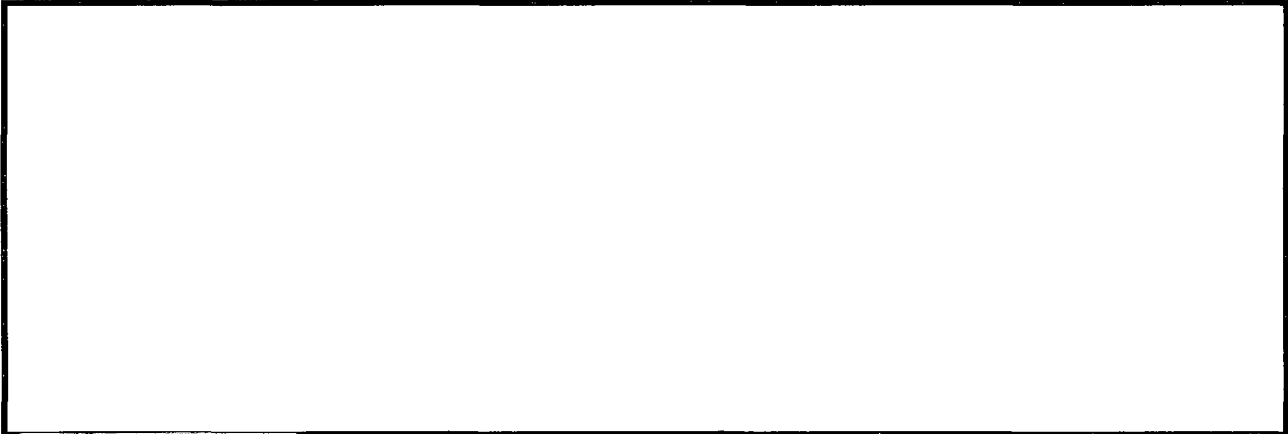
The DCS3000 system employs McAfee VirusScan anti-viral software.

4.5. Maintenance

The DCS3000 Users' Guide includes maintenance procedures that include preventive maintenance, scheduled to maximize the availability of the system, and thus to minimize interference with the operation of the system. TICTU provides on-call maintenance support of fielded systems.

5. SECURITY

5.1. System/Facility Access



b2
b7E

FBI system users receive background checks based on their job function before they acquire system privileges in accordance with the FBI personnel policy. Non-Bureau personnel who are required to perform maintenance on DCS3000 within a central monitoring plant (CMP) may be approved for escorted access based on an FBI-conducted Limited Background Investigation.

5.2. Physical Environment

DCS3000 systems physically reside in FBI field offices within CMPs. Because the DCS3000 resides in the field offices, access to CMP housing the system is restricted to authorized personnel only. Central monitoring plants are locked at all times and controlled by a variety of access control devices and procedures. Authorized personnel escort any unauthorized personnel (e.g., maintenance personnel, facility support contractors) in order to monitor their activity while in the CMP.

5.3. Data Storage Media

Though the primary function of this system is not data storage, it does store some data temporarily before it is collected by the Multiserver and forwarded to the client. Call data is

provided from the switch to the VanGuard and temporarily stored until the MultiServer collects it and sends it to the client.

5.4. Backup and Recovery

The DCS3000 provides a capability to conduct backup storage and restoration of data and access controls. The DCS3000 Users' Guide includes recovery procedures that assure that system recovery is done in a trusted and secure manner.

The DCS3000 backup capability provides for the restoration of any security-relevant segment of the system state (e.g., access control lists, cryptologic keys, deleted system status information) without requiring destruction of other system data.

6. POINTS OF CONTACT

[Redacted]

DCS3000 Program Manager

FBI Investigative Technology Division (ITD)

FBI Engineering Research Facility (ERF)

Tele. No. [Redacted]

b6
b7C

[Redacted]

Senior Systems Analyst (Contractor) and ISSO

ITD/ERF

Tele. No. [Redacted]

~~SECRET/NOFORN~~
WORKING PAPERS

Review of CSOC SSP compared to Certification Test Reports

Section 3.5.1 – has the system classifications as UNCLASSIFIED/FOUO/SBU/NOFORN but NO SECRET, however, the overall classification of the document is ~~SECRET/NOFORN~~

Section 3.6.1 - Over-classification - The SSP classifies as ~~SECRET/NOFORN~~
Section 3.7 describes Tier Description as ~~SECRET/NOFORN~~
Section 3.8 System mode of operation is classified as ~~SECRET/NOFORN~~

b2

Section 7.4.1 - States that Active Directory is not implemented on the system, however, I believe what is intended is on the low-side AD is not implemented but on the High-Side AD is activated and Kerberos is operational ONLY on the High-Side.

Section 7.5.8 – System Start-Up – CSOC servers are configured to be started cold without admin input, start without users being logged in.

Privileged Users Guide

Paragraph 7.3.5 – Technical Access Mechanisms – Screen savers lock requires a password, conflicts with Section 12 Exception; the CSOC does not utilize Screen Lock on monitors per the SSP

Section 7.28 – states lockout after 3 tries but CTR references 4 tries

SSP conflicts with Users Guide

- a. 3 tries for lock out – SSP states 4 tries as does CTR
- b. Kerberos policy needs to be defined between the two sides of the system; high-side uses Kerberos but the low-side do not have Active Directory activated and cannot use Kerberos.

Tier EC – level of concern, mode of operation, and tier level are all UNCLASSIFIED but the SSP classified all these levels at ~~SECRET/NOFORN~~

Certification Test Report – Low-Side Comments

	Comments
AC-5.3.4 Pass	Screen Saver not used – exception to policy per SSP section 12
AC-5.3.5 Pass	No admin required to start servers, servers are set to start without any user interface
AC-5.3.12 Pass	Kerberos – SSP 7.4.1 Do not implement Active Directory- cannot use Kerberos w/o AD being applied to the operating system

~~SECRET/NOFORN~~
WORKING PAPERS

1

~~SECRET/NOFORN~~
WORKING PAPERS

I&A 3.2.1 Pass unique users; SSP 7.5.8 servers start up without any user interface

DT 2.2.1 Pass Kerberos – will not work w/o AD being activated

Comments from the CSOC SSP

(U) Related to the classification of data on the CSOC system; paragraph 3.1 of SSP states:

(U) Health and welfare plus allows CSOC through Unicenter software, also provides HELP DESK functions, system troubleshooting and environmental monitoring.

- a. Help desk functions to all Field Offices with collection systems.
- b. Remote trouble shooting and resolution of identified system problems.

The following sections were not marked with section classification markings:
3.9; 3.9.1; 3.9.3; 3.9.5; 3.9.7; 3.9.8; 3.9.9;

(U) Section 3.9.9 states this system does not store or process data stored on any other system. Question: how can CSOC perform help desk and troubleshooting the other systems without being able to access the data and store the information on the system?

(S/NF) Services all MS File Sharing; Kerberos; SNMP; Telnet; FTP, HTTP;
TCP/UDP/ICMP

(S/NF) paragraph 7.2.6 – Users can change Passwords whenever, they want to, however the block for 3 months was checked.

(U) Paragraph 8.2 – A privileged user's guide is available
There are apparently normal users generated on the CSOC system; however, only a privileged user's guide is generated. Section 7.2.1 – Page 14 -Users are assigned individual accounts and passwords normally its regional managers.

Section 12 EXCEPTIONS

No Screen savers will be used in the CSOC system

(U) Appendix A to the Privileged Users Guide

(S/NF) Remote Admin Client (ITDRAC) remote capability for the DSMs, to port patches and provides general system administration over the network. ITD Client is the remote admin for DCS 5000.

(S/NF) Section 7.6.6 Audited Activities

No auditing for either success or failure for

- Information Downgrades or overrides
- Copying data to re-moveable media

~~SECRET/NOFORN~~
WORKING PAPERS

(U) Appendix B to the Privileged Users Guide

(S/NF) No remote access on the unclassified side

7.4.2 Monitor – Kerberos and a trusted path, however Active Directory is not utilized on the Low-Side therefore Kerberos will not function in a Windows based operating system.

(S/NF) 3.1.3 No IDS on the CSOC System

The server settings state that the Guest account was renamed to XGUEST; however the account was set to 0 or disabled.

01/23/2006

[redacted] We had a meeting with [redacted] from CU Testing on Friday 01/20/2006, and he was quite adamant that the CSOC system was only a health and welfare system, however, after reviewing the SSP in depth and talking to [redacted] on January 23, I confirmed that the CSOC system is in fact a full blown help desk and troubleshooting system in addition to the health and welfare functions as tested. I asked [redacted] several times if the CSOC turned out to be a help desk and troubleshooting system to the DCS-5000 would that modify there testing in anyway, and he continually stated it would not.

b6
b7C

COMMENT:

I would think that at a least some additional testing should be conducted to ensure that no residual collection data is being maintained by the CSOC system. Based on the facts surfaced I would not agree to the CSOC system data being downgraded to SBU, but must stay at ~~SECRET/NOFORN~~ based on the level of support rendered.

For Official Use Only

SECURITY EVALUATION REPORT

FOR THE

DCS3000

MARCH 27, 2003

Prepared by:

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-25-2007 BY 65179/DMH/KSR/LMF

For Official Use Only

For Official Use Only

INTRODUCTION

There is risk in any endeavor. One of the ways to cost effectively preserve assets is to manage risk. Managing risk entails accounting for assets and how to protect them. The following is an analysis of the certification documentation to include the Statement of Residual Risk for the DCS3000. The Security Evaluation Report (SER), examines the nature of the DCS3000, the inherent risks, mitigating strategies, recommended countermeasures (if any), security safeguards in use and subsequent residual risk to the system. The SER provides information to the Designated Accrediting Authority (DAA) regarding the overall security posture of the system. Based on the analysis, the DAA Representative makes a recommendation to the DAA for an accreditation decision.

1. Background

The DCS3000 is an electronic surveillance (ELSUR) collection system that supports criminal law enforcement (CLE) Title III criminal investigations. It is modular, therefore it is set up for each case. The dataflow occurs in the following manner:



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 and the only network connectivity with the TSP.

DCS3000 data is collected in support of criminal cases and is protected as evidence. If this data is inappropriately divulged, the certifier stated that it may cause a loss of life. Therefore, a *Medium* level of concern was assigned for Data Confidentiality by the certifier. However, since the certifier assigned this level of concern, the most recent version of the FBI C&A Handbook elevated the loss of confidentiality where data compromise could "... lead to personnel safety (*sic*) or loss of life, if disclosed; human sources (informants, assets, cooperating witnesses) would be placed in compromising situations if information was disclosed . . ." to a *High* level of

For Official Use Only

concern. Therefore, the DAA Representative has conducted this evaluation accordingly.

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. Additionally, lost or altered audio data could jeopardize undercover law enforcement personnel lives and activities, according to the SSP. Therefore, a *Medium* level of concern was assigned for Integrity by the certifier. The current version of the FBI C&A Handbook has elevated possible loss of life to a *High* level of concern. The DAA Representative has conducted this evaluation accordingly.

During an investigation in which the DCS3000 is used, it is critical that the system is available at all times to record data. If the system becomes unavailable for any reason, law enforcement personnel lives and the cases can be put in jeopardy. Lack of availability would impact the organizational mission, rather than National Security interests. For these reasons, a *Medium* level of concern has been assigned for Availability by the certifier, according to the FBI C&A Handbook.

The following evaluation is based on the DCS3000 System Security Plan (SSP) and Risk Report dated December 17, 2002 and received a second time by the Accreditation Unit March 25, 2003.

2. Evaluation of C&A Package

The certifiers approached the system as a Tier 2 and security testing was performed. Below is a description of some of the security safeguards for the DCS3000:

The Information System Security Officer (ISSO), which has overall system security responsibility for the secure installation, performance and day-to-day operation, has been assigned to [REDACTED]. Each field office with the system should have an ISSO. There is separation of duties between system (Users) and security system administration.

b6
b7C

The operating system used, Windows 2000, is listed on the EPL (Evaluated Products List) and evaluated at the C2 level. I&A, Object Reuse and Audit are implemented by Windows 2000 operating system. The system is configured before deployment.

Virus DAT files are updated as they become available, or immediately after a collection effort has been completed. Removable media is scanned before transferring data to the Telephone Application (TA) on FBINET.

The DCS3000 routers, servers and terminals included in this evaluation are located in FBI controlled spaces or when co-located, controlled by FBI personnel. All personnel having access to the DCS3000 operations within FBI controlled spaces have at least Secret clearances. If the

For Official Use Only

For Official Use Only

collection effort and supporting court order are non-DOJ and not controlled by FBI personnel, they are obligated to comply with "Attorney General Guidelines for Loan of Technical Equipment."

3. Statement of Residual Risk

Accreditation is the formal declaration by the accrediting authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards. Part of the accreditation process is the acceptance of a given level of risk against a defined threat. The accrediting authority must balance:

- the risk of disclosure, loss or alteration of information;
- the availability of the system based on the vulnerabilities identified by the certification process;
- the threat that these vulnerabilities may be exploited in the specific environment in which the system is being used; and
- the operational needs and benefits associated with the system under evaluation.

The following is a summary of the security issues and mitigation factors which were identified through the risk analysis, certification activities and accreditation review. The certifiers considered the following to be of Medium risk. With proposed mitigating strategies in place, the overall risk to the system will be Low.

Vulnerability 1: *Accounts locked due to successive logon failures are locked for 30 minutes instead of forever, as required. An unauthorized user could try four times, every 30 minutes, to guess a password.*

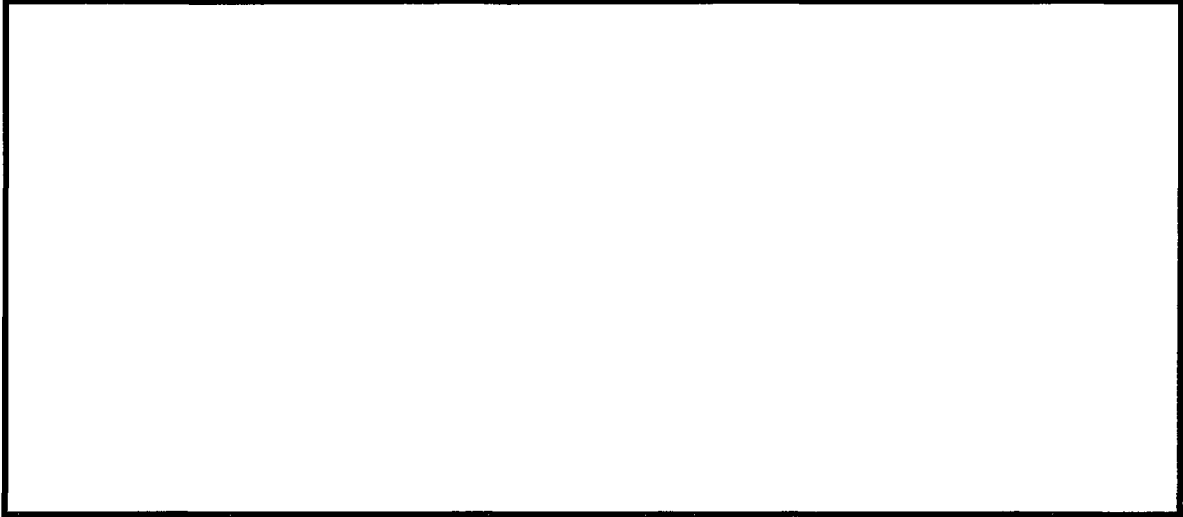
Risk Impact: There is a potential for a user to access evidence surreptitiously.

Current Mitigating Factors: There is no remote access to the servers and clients. Therefore, all system access requires physical access to the terminals. Physical access to a collection site is controlled. It would take a considerable amount of time to crack a password. This increases the likelihood of discovering unauthorized activity. Additionally, it would probably be easier to look over a user's shoulder and steal a password. The thirty minute lockout is a reasonable deterrent to unauthorized use, while permitting continuous monitoring. The risk is assessed as LOW.

Recommended Countermeasure: As users need constant access for collection and monitoring activities, a thirty minute lockout is sufficient to deter unauthorized access in an FBI controlled space, yet allow valid users to perform their work. The DAA Representative recommends granting a policy exception in this instance.

For Official Use Only

For Official Use Only



b2
b7E

Vulnerability 3: *There are no documented procedures for the retention or review of the audit logs.*

Risk Impact: Security relevant events could go undetected. Audit logs could be overwritten and evidence to trace user actions could be lost.

Current Mitigating Factors: The Windows 2000 OS security audit log is enabled with the correct settings when deployed. There are a limited number of users at each deployment. The risk is assessed as MEDIUM.

Recommended Countermeasure: Develop audit review and retention procedures for each deployment at sites where the FBI is a participant.

4. Recommendation

The DCS3000 was assessed by the certifier as a Tier 2, Protection Level 1 system. Levels of concern for Availability, Integrity and Confidentiality were assessed as Medium by the certifier. The DAA Representative elevated levels of concern for Integrity and Confidentiality to High, based on the rationale presented in Section One. It is recommended, by the DAA Representative, that the DCS3000 be accredited at the SBU level with a Dedicated Security Mode of Operation for three years.

For Official Use Only

For Official Use Only

Audit review and retention procedures should be developed and implemented within 180 days. After the 180 days, it is recommended that the Information Technology Systems Unit (ITSU) provide a formal notice that the countermeasure has been enacted and verified. If, after 180 days, formal notice has not been received, the DAA Representative will recommend rescinding the accreditation. Additionally, the DAA Representative emphasizes the importance of scanning all media for malicious code with current virus scan DAT files after copying from the DCS3000 and before uploading into the TA on FBINET.

For Official Use Only