Freedom of Information and Privacy Acts

FOIPA# 1056287 and FOIPA#1056307-1

Subjects: DCS-3000 and RED HOOK

File Number: DIVISION CD'S

Section: 13

Federal Bureau of Investigation

~~SECRET~~

For Official Use Only

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

Certification and Accreditation Status

Status	TS/SCI	TS	S	C	SBU	UND	*Totals*
Accredited	10	1	35		31		77
Accredited w/ Action Plan	4		13		6		23
Certified/Undergoing Accred			9		6		15
IATO	2		6		4		12
Registered	2		6		22	7	37
Research					1	4	5
Undergoing Certification	8	1	30		50	4	93
Totals	**26**	**2**	**99**		**120**	**15**	**262**

System	*Classification*	*CUST*	*Approval*	*Granted*	*Expires/ or ROC*	*Effort Type*	*Cert Team*	*Effort Status*	
Administrative Mainframe Applications (Admin MF Apps)	Secret	ITOD	Operate	12-Jul-01	11-Jul-04	Reaccred Original	CU CU [redacted]	Undergoing Certification Accredited w/ Action Plan	b6 b7C
Annual Field Office Report (AFOR)	Secret	CTD	Operate	09-Apr-02	09-Apr-05	Original	CU[redacted]	Accredited w/ Action Plan	
Anti-Drug Network (ADNET)	Secret	CCD	Operate	08-Mar-05	07-Mar-08	Reaccred Original	CU CU [redacted]	Accredited Accredited	
Application Server Farm (ASF) (aka Mini-Server Farm)		Secret	ITOD	Interim	30-Sep-04	29-Mar-05	Original	CU-[redacted] IATO	b6 b7C
Asset Validation Laptop	Secret	CD				Original	ITSU[redacted]	Undergoing Certification	
Automated Booking System (ABS)	Sensitive But Unclass	CJIS	Operate	27-May-03	26-May-06	Original	CU-[redacted]	Accredited	
Automated Travel Remittance Service (ATRS)	Undetermined	FD	None			Original	CU-[redacted]	Registered	
Background Investigative Contract Services (BICS On-Line)	Secret	ASD	Operate	24-Oct-02	23-Oct-05	Original	CU-[redacted]	Accredited	
Biometric Solicitation Reviewers (BSR)	Undetermined	ITD	None			Original	ITSU-INDUSTRIAL	Registered	
BlackBerry Wireless Email System	Sensitive But Unclass	ITOD				Original	ITSU[redacted]	Undergoing Certification	b6
Bomb Scene Response and Reporting Kit (BSRRK) Registered (aka COBRA)		Sensitive But Unclass				LAB	Original	ITSU[redacted]	b7C

For Official Use Only

DATE: 05-21-2007
CLASSIFIED BY 65179 DMH/TAM/KSR/JB
REASON: 1.4 (g)
DECLASSIFY ON: 05-21-2032

#1056287-000 (1)

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

System	Classification	CUST Approval	Granted	Expires/ or ROC	Effort Type	Cert Team	Effort Status
Cyber Security Assessment and Mgt Tool-Trusted Agent (CSAM-TA) (aka FISMARS)	Secret	SecD			Original	CU[redacted]	Undergoing Certification
CYBERTRANS II	Secret	OIO Operate	14-Jun-04	13-Jun-07	Original	CU[redacted]	Accredited
(S) [redacted]	Top Secret SCI	ITD Operate	27-Feb-03	27-Feb-06	Original	CU[redacted]	Accredited
Data Collection System 3000 (DCS 3000) (aka CALEA Accredited (Communications Assistance to Law Enforcement Act))		Sensitive But Unclass	ITD	Operate	29-May-03	28-May-06	Original CU[redacted]
Data Collection System 5000 (DCS 5000)	Secret	ITD			Original	CU[redacted]	Undergoing Certification
Data Collection System 6000 (DCS 6000) (aka Digital Accredited w/ Action Plan Storm)		Sensitive But Unclass	ITD	Operate	30-May-03	29-May-06	Original CU[redacted]
Data Extraction & Extension Project (DEEP)	Secret	CTD Operate	07-Feb-05	07-Feb-08	Original	CU[redacted]	Accredited w/ Action Plan
(S) [redacted]	Top Secret SCI	CD Operate	18-Oct-04	17-Oct-07	Original	CU[redacted]	Accredited w/ Action Plan
DEG Dedicated Controllers	Sensitive But Unclass	ITD None			Original	CU[redacted]	Undergoing Certification
Demon	Undetermined	ITD			Original	CU[redacted]	Undergoing Certification
Denver Sq13 Internet Network	Sensitive But Unclass	DN			Original	ITSU -[redacted]	Registered
Dept of State C-LAN (DOS C-LAN)	Undetermined	CTD		30-Jun-04	Original	CU-[redacted]	Research
Digital Collection Systems Network (DCS Net)	Sensitive But Unclass	ITD Operate	04-Feb-05	04-Feb-08	Original	CU-[redacted]	Accredited w/ Action Plan
Digital Document Management System (DDMS)	Secret	LAB Operate	18-Oct-04	17-Oct-07	Original	CU-[redacted]	Accredited w/ Action Plan
DirectorNet	Secret	ITD			Original	CU-[redacted]	Certified/Undergoing Accred
DNA Local Area Network (DNA LAN)	Sensitive But Unclass	LAB Operate	24-Oct-03	24-Oct-06	Original	CU-[redacted]	Accredited
Document Capture System (DocLab2) (aka DCS)	Secret	RMD			Original	CU-[redacted]	Undergoing Certification
Document Control System (DCS)	Secret	RMD Operate	09-Apr-03	09-Apr-06	Original	CU-[redacted]	Accredited
DOORS	Secret	INSD Operate	04-Feb-05	04-Feb-08	Original	CU-[redacted]	Accredited w/ Action Plan
(S) [redacted]	Top Secret SCI	CD Operate	26-Mar-02	26-Mar-05	Original	CU-[redacted]	Accredited w/ Action Plan
Electronic Key Management System (EKMS)	Secret	SecD Operate	22-Apr-02	21-Apr-05	Original	ITSU -[redacted]	Accredited w/ Action Plan
Electronic Process Auto Syst (Confidential) (EPAS) Certification (aka E-Work)		Sensitive But Unclass		FD	09-Feb-05	Original	CU[redacted] Undergoing

b1
b2
b6
b7C
b7E

b1
b2
b6
b7C
b7E

System Security Plan (SSP)
Appendix F - Certification Pre-Test Results
for the DCS 3000

Prepared by:
Certification Test Team
[redacted]

b6
b7C

~~Derived From: FBI Classification Guide G3, Dated 1/6/1997~~
~~Declassify on: X1, X6, X7~~

August 27, 2002

Table of Contents

1.0 CERTIFICATION RESULTS

(U) ~~(S)~~ Based on the certification review of the DCS 3000, several significant information assurance deficiencies were found. 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.

(U) ~~(S)~~ The major deficiencies were in the areas of [redacted] b2 b7E

(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.

(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.

1.2.1 Technical Findings

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

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

b2
b7E

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

No.	Major Security Findings	Test Case	Scan Report
6 (U)	~~(S)~~ [redacted]	VS-03	Users.txt

b2
b7E

No.	Major Security Findings	Test Case	Scan Report
ISS System Scanner			
1.(U)	(X) [redacted] Th[redacted]key is set [redacted] *Set permissions as follows:* [redacted]	VS-01	Workstation Vulnerabilty Report page 1

b2
b7E

b2
b7E

No.	Major Security Findings	Test Case	Scan Report
2. (U)	~~(S)~~ [redacted] CAUTION: If the Interactive user does not have write permission at the root key, then ordinary users will not be able to install applications that expose DCOM objects.	VS-01	Pages 3-5, 7, 20, 26 of Workstation Vulnerability Report . b2 b7E

No.	Major Security Findings	Test Case	Scan Report
3. (U)	~~(S)~~ [redacted] The [redacted] key is set [redacted] [redacted] [redacted] [redacted] [redacted]	VS-01	

b2
b7C

b2
b7E

b2
b7E

No.	Major Security Findings	Test Case	Scan Report
4. (U)	~~(S)~~ [redacted] The [redacted] key is set [redacted] [redacted] [redacted] [redacted] [redacted]	VS-01	Pages 2- 3 of Workstation Vulnerability Report . b2 b7E

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

CISCO Secure Scanner			
1 (U)	~~(S)~~ [redacted]	NS-CS-01	CSS Vulnerability Report
2 (U)	~~(S)~~ [redacted]	NS-CS-01	CSS Vulnerability Report

Operating System Manual Testing

b2
b7E

1. (U)	~~(S)~~ [redacted]	SI-03	Refer to page 23 of this document.

1.2.2 Procedural/Policy Findings

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

None found.

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	

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.)

(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	

(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	

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	

(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:

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)(c)**: When inoperable diskettes tape cartridges printouts ribbons and similar items used to process sensitive or classified information must be destroyed in accordance with MIOG Part II Section 26.		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	

(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} ~~(S)~~ 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

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

(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 t[redacted] backups are handled centrally by FBI on FBINET..
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.

b6
b7C

(U) Pass/Fail:

Requirement	Pass/Fail	Comment
(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: 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.	Pass	
DCID 6/3 Doc 1: Documentation shall include: 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.	Pass	
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.	Pass	

Requirement	Pass/Fail	Comment
DCID 6/3 Doc3: The DAA may direct that documentation also shall include: Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level. Reports of test results. 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.	Pass	
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.	N/A	
(U) **DOJ 2640.2D 9.1.** [Components shall:] Develop a contingency plan for each general support system and major application. Contingency plans shall: (1) Identify the priorities of the system for restoration, taking into consideration the system's role in fulfilling Department mission and interdependency requirements. (2) Determine the maximum amount of elapsed time permissible between an adverse event and putting the system's contingency plan into operation. (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). (4) Identify interdependencies with other systems (i.e., other component, Federal, State or local agencies) that could affect contingency operations. *(5) Identify system owners, roles, and responsibilities.*	Pass	

Requirement	Pass/Fail	Comment
(U) **DOJ 2640.2D 9.2.** [Components shall:] Develop and maintain site plans that detail responses to emergencies for IT facilities.	Pass	
(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.	Pass	
(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.	Pass	

(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	
DCID 6/3 Integrty2: Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g., integrity locks, encryption).	Pass	

Requirement	Pass/Fail	Comment
DCID 6/3 Integrty3: Integrity, including the implementation of specific non-repudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.	N/A	

(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	

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.

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.

(U) Pass/Fail:

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

(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.

(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	

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) Requirements:

(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.

(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.

(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.

(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.

(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.

(U) **DOJ 2640.2D 38.** Until reliable executable content scanning technology is available to address security concerns with regard to mobile code or executables obtained via the Web, the following shall apply:

DOJ 2640.2D 38.a. All mobile code or executable content employed within a Department intranet shall be documented in the system security

plan and approved by the DAA.
DOJ 2640.2D 38.b. As feasible, components shall implement a code review and quality control process for deployed mobile code or executable content.
DOJ 2640.2D 38.c. For those instances where there is no operational need to download mobile code or executable content, the IT system shall be configured to prevent the downloading of mobile code or executable content.
DOJ 2640.2D 38.d. Downloading of mobile code and executable content from a controlled interface between interconnected systems shall be permitted only when a boundary protection device appropriately configured (to handle such a download) and is in place and approved by the DAA.
(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.

(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.

(U) <u>Preparation</u>: 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) ~~(S)~~

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.

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) ~~(S)~~ Analysis of Results:

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	

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	

(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:

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	
(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	

Requirement	Pass/Fail	Comment
(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	

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.

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

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome
1	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). Observe the objects located under Computer Configuration/Windows Settings/Security Settings.			Security Settings objects should include: Account Policies Local Policies IP Security Policies (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).	As expected.
2	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.		**Password Policy**		
			[redacted]	[redacted]	NO password history.
			[redacted]	[redacted]	As expected
			[redacted]	[redacted]	Currently set to zero days.
			[redacted]	[redacted]	Currently set at zero characters
			[redacted]	[redacted]	As expected

b2
b7E

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	forever (sysadmin must provide new password)	No account lockout
			Account lockout threshold	3 invalid logons	Not enable due to the previous finding.
			Reset account lockout counter after (time)	Not defined	Previous findings indicate this test element is not instituted.
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.

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 excepted

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 webservers 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.)	THe following group and users are allowed to logon locally: Backup Operators Power Users Users Admin Guest
			Manage auditing and security log	Admin	As expected

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

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

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**		
			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.

Step	Procedure	Date Tested	Test Element	Expected Outcome	Actual Outcome
			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	

(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): [redacted] [redacted]	Fail	[redacted] b2 b7E

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	

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	b2
[redacted]	Pass	b7E
[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	

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.

(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

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. For Windows NT/2000 workstations, press simultaneously CTRL, ALT & DELETE to view the Windows NT security dialog box. Click on the Change Password button to view the Change Password dialog box. Select the correct domain. For other workstation operating systems, use appropriate dialog to change passwords. Enter the current password in the old password field. Enter and confirm new passwords as follows: [redacted] Enter a valid new password and confirm it.	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

Step	Procedure	Expected Outcome	Date Tested	Actual Outcome
3	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: [redacted]	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. The following should be found for Windows 9x and NT: [redacted] The following value should be found for Windows 2000: 0	8/23/02	As expected. b2 b7E b2 b7E

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

(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: [redacted]	Fail	[redacted] b2 b7E

Digital Collection System Network (DCSNET)
System Security Plan (SSP)

System Designator: N/A

30 January 2004

Version: 1.0

(1)

Table of Contents

Error! No table of contents entries found.

Record of Changes

Number	Date	Description	Entered By

1.0 Introduction

This System Security Plan (SSP) documents the security policies and procedures for the DCSNET information system at Quantico. This plan establishes the approved operational baseline and configuration and is the basis for certification and accreditation of DCSNET.

1.1 Security Administration

1.1.1 System Information

Information System Name	DCSNET
Information System Number	N/A
Date of Plan	1/30/04
Revision/Version	
TSABI Number	N/A
Web Location for Documentation	N/A
Status	
Project ID	N/A
Deployment Installation Date	
Certification Test & Evaluation Date	
Required Operational Date	

1.1.2 Key System Points of Contact

System Owner	Name	[redacted]
	Organization	FBI/TICTU
	Commercial Phone:	[redacted]
ISSO	Name	[redacted]
	Organization	FBI/TICTU
	Commercial Phone:	[redacted]
System Administrator	Name	[redacted]
	Organization	FBI/TICTU
	Commercial Phone:	[redacted]
Certification Team Lead	Name	[redacted]
	Organization	Security Division/IAS/CU
	Commercial Phone:	[redacted]
Security Certification Official	Name	[redacted]
	Organization	Security Division/IAS/CU/Unit Chief
	Commercial Phone:	[redacted]

b6
b7C

Certification Official	Name	Dean Hall
	Organization	Security Division/IAS/Section Chief
	Commercial Phone:	[redacted]
DAA Representative	Name	[redacted]
	Organization	Security Division/IAS/AU
	Commercial Phone:	[redacted]

b6
b7C

1.1.3 Security Organization

The Switch-Based Intercept Team within the Telecommunications Intercept and Collection Technology Unit (TICTU) oversees all administration and security concerns for the network. See Attachment A for an organizational chart.

1.2 Mission

The mission of the FBI's TICTU is the development, deployment, and support of access and collection technology to perform lawfully authorized electronic surveillance (ELSUR) of telecommunications services. The TICTU is responsible for providing equipment to the field, troubleshooting problems with equipment and systems, providing training to field office users, tracking needs of the field to identify new ELSUR requirements, and serving as the FBI's technical liaison with telecommunications service providers. .

1.2.1 Purpose and Scope

The Digital Collection Systems Network (DCSNET) is a transport mechanism for moving CALEA CDC and streamed CCC data from the service provider sources to the proper FBI Field Office destinations

1.2.2 Supported Projects

Project Name	Classification & Compartments	Project POC
DCS-3000	Unclassified	[redacted]

b6
b7C

1.2.3 Information System Usage

□ Briefing Boards
□ Communications
□ Collaborative Computing
□ Database
□ Data Release
□ Email
□ Image Processing
□ Mapping

□ Network Management
□ Presentations
□ Software Development
□ Prototyping
□ Signals Processing
□ Spreadsheets
□ Web
□ Word Processing

☒ Other:

Data Transmission

2.0 Secure Facility Description

2.1 Facility Layout

DCSNET routers will be housed in each of the Field Offices.

2.2 System Layout

Facility drawing will be requested from each office as the routers are installed. These drawings will be put into Attachment B in this document.

2.3 Physical Environment

Is the secure facility accredited or approved to process and store information at the level covered by this SSP?	□ Yes □ No
Who accredited or approved the facility?	
Provide CITE Nbr & DTG or Date of approval letter.	
State the classification and level (compartment) approved for the facility.	□ Secret □ SCI Others: □ Top Secret □ SI ______ □ TK ______ ______
Is the system approved for unattended processing?	□ Yes □ No
Is the facility approved for 24-hour operation?	□ Yes □ No
Is the facility approved for Open or Closed storage?	□ Open storage □ Closed storage
Items approved for Open Storage	[List]
Items restricted to Closed Storage	[List]
Are classified and lower classified systems co-located within the facility? If "YES", provide a narrative below discussing the separations between the systems.	□ Yes □ No

2.3.1 Access to Physical Environment

2.3.2 Separation of SCI and Unclassified Systems

DCSNET equipment is unclassified and is not collocated with classified equipment.

2.4 TEMPEST

N/A

3.0 System Description

3.1 Summary

The [redacted] consists of Cisco 2610XM routers, running Cisco IOS 12.2(15), that connect the Field Offices together through a [redacted] network backbone. b2 b7E

3.2 System Diagram

The [redacted] is made up of T1 connections to each field office from [redacted] private (not internet connected) backbone. The fully meshed nature of this arrangement allows each field office to connect directly to every other field office, thus increasing the speed and reliability of the network. [redacted] backbone employs the MPLS VPN protocol to ensure that FBI traffic is separated from all other traffic on the backbone. The FBI controlled routers use IPSEC AES encryption to further secure the data. See Attachment C for a Network Block Diagram.

3.3 Personnel Security

Only administrators within TICTU will directly access the routers.

3.4 Non-US Citizens

3.5 Data Processed

3.5.1 Classification and Compartments

☒ Unclassified	□ SI
□ Confidential	□ TK
□ Secret	□ B
□ Top Secret	□ G
□ Other: ____________ ____________	□ Other: ____________ ____________

3.5.2 Dissemination Controls

□ For Official Use Only	□ ORCON	☒ SBU
□ NOFORN	□ TK	☒ LES
□ Rel To: ____________ ____________	□ Other: ____________	

3.6 Confidentiality, Integrity, and Availability Goals

Confidentiality

☐ Basic ☐ Medium ☒ High

Integrity

☐ Basic ☒ Medium ☐ High

Availability

☐ Basic ☒ Medium ☐ High

3.7 Tier Designation

☐ Tier 1 ☒ Tier 2 ☐ Tier 3 ☐ Tier 4

3.8 System Concept

☒ Dedicated ☐ Compartmented

☐ System High ☐ Multi-Level

3.9 Interconnection Interface Description

3.9.1 Direct Network Connections

___ This system does not connect with any other system.

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

System Name	Classification & Compartments	Accredited By
DCS-3000	Unclassified	

3.9.2 Connectivity Management Procedures

Field Office requests for connectivity to DCSNET are made to the DCSNET system owner. The system owner, currently [redacted] determines the appropriateness of the request. If approved, the system owner tasks the system administrator and ISSO to coordinate the new installation. b6 b7E

3.9.3 Interconnection

The DCSNET router connects to a switch or hub that is part of the DCS-3000 system. Both systems are unclassified, so no Controlled Interface is required.

3.9.4 Connectivity Procedures

3.9.5 Controlled Interface Requirements

DCSNET will only connect with systems of equal classification and will not require controlled interfaces.

3.9.6 Data Flow Diagram

3.9.7 Telecommunications Security

The routers encrypt the data transmitted over the DCSNET using IPSEC AES encryption algorithms. The routers use a pre-shared encryption key that is changed every 6 months.

3.9.8 Networking

___	LAN Type:		Topology:	___	NSC Line Filter
	Speed:		Cabling:	___	Apple Local Talk cabling
___	Router	Make:	Model:	___	Fiber optic cabling
	O/S Version:			___	FDDI
___	Hub	Make:	Model:	___	ATM
	O/S Version:			___	Cabling located in conduit
___	Bridge	Make:	Model:	___	Plenum rated cabling: Location:
	O/S Version:			___	Other: ____________
___	Modem	Make:	Speed:	___	Other: ____________

3.9.9 Indirect Connections

_X_ This system does not accept or process data stored on any other systems.

___ This system accepts and processes data stored on media created by with the following network(s) or system(s):

System Name	Classification & Compartments	Accredited By

_X_ This system does not share or distribute data to any other systems.

___ Data stored on media created or used on this system is distributed for use by the following network(s) or system(s):

System Name	Classification & Compartments	Accredited By

4.0 Hardware

4.1 Hardware Listing

The equipment used for DCSNET are all Cisco 2610XM routers with 96MB Flash memory. See Attachment E – Equipment List for full list with locations and serial numbers as they are installed to the field.

4.2 Custom-Built Hardware

4.3 Configuration Management

See paragraph on the 7.5.3 Configuration Management Program

5.0 Software

5.1 Software Listing

Vendor	Software	Version
Cisco	IOS	12.2(15)

5.2 Configuration Guides

5.3 Allowed Services and Protocols

5.3.1 Internal

The routers do not filter any ports or protocols for the data passing through the DCSNET.

5.3.2 External

SSH is enabled on the routers for remote management.

5.3.3 Protocols

The routers do not filter any ports or protocols for the data passing through the DCSNET.

5.4 Mail System

There is no Mail system on DCSNET.

5.5 Foreign Software

There is no foreign software used on DCSNET.

5.6 Software with Restricted Access or Limited Use Requirements

Configuration software to manage the Cisco routers and VPN configuration requires use of an administrator password. This password is not stored in plaintext and is not displayed in plaintext within the configuration file.

5.7 Configuration Management

See paragraph on "7.5.3 Configuration Management Program"

6.0 Data Storage

No data is stored on the routers. The routers contain a flash memory for configuration files.

6.1 Media Types

None

6.2 Media Handling

No media is used within DSCNET.

6.3 Backup and Restoration Process

The administrators in Quantico will maintain copies of the configuration files for each router. These copies will be obtained through the network using SSH.

6.4 Backup Protection

6.5 Disaster Recovery

7.0 Security Requirements

7.1 Threats & Vulnerabilities

7.2 User Access and Operation

DCSNET does not support individual general users. Only administrative users have access to DCSNET. All access controls listed in Section 7.2 and its subsections pertain do administrative/privileged users only.

7.2.1 Access Controls

Access will require a username and password. A second password will be required to enter the administrator mode.

7.2.2 Account Procedures

Administrators are given a userID and password for basic access to the router, based on a justified need. Once personnel have gained formal approval to access systems within TICTU, approval for DCSNET administrative access is based on the discretion of the system owner.

7.2.3 Authenticator Procedures

7.2.4 System Users

There are no general system users.

7.2.5 Privileged Users

____ All privileged users have their own unique UserID and unique password.
__X_ Some privileged users share a UserID and password. (Explain below)
____ Some privileged users share a password. (Explain below)

Due to the design of the software, there can only be one password to enter the administrator mode.

7.2.6 Password Changes

Password will be changed every 6 months.

7.2.7 Password Generation

Passwords are generated by the administrators.

7.2.8 Log-on Error Handling

Administrators will be given 3 attempts to login to the router before their SSH session is terminated.

7.2.9 Account Lockout Handling

Due to the undesirability of administrative accounts being locked out, the routers do not support this feature.

7.3 User Groups and Access Rights

7.3.1 User Groups

All users are administrators.

7.3.2 Non-data File Access

All administrators can change the configuration files.

7.3.3 System Access Rights

All users are administrators.

7.3.4 Audit Logs

7.3.5 Privileged Users

7.3.6 Privileged Users Guides

7.3.7 Technical Access Mechanisms

Administrative access to router information and configuration requires the use of two passwords; one which is unique to the individual administrative users, and another common password which allows access to change the configuration of the router.

7.3.8 Discretionary Access Control

N/A

7.3.9 Need-to-Know Controls

N/A

7.3.10 Mandatory Access Controls

N/A

7.3.11 Discretionary Access Control Augmentation

N/A

7.4 Security Support Structure Protection

7.4.1 General

System access requires physical access to a node on the network. All network nodes are located in physically secure areas.

7.4.2 Trusted Communications

N/A

7.4.3 Validation Procedures

The procedures followed to validate the security posture of DCSNET can be found in Attachment I – DCSNET Certification Test Plan.

7.5 Security Features and Assurances

7.5.1 Incident Reporting

7.5.2 Remote Access

Remote access is allowed through the network using SSH. Administrators can login with a username and password.

7.5.3 Configuration management Program

The administrators handle configuration management. Administrators will setup new routers using a baseline configuration that contains all the security features. Changes to any router configurations are logged in a database maintained at Quantico. All DCSNet system changes are approved by the Network Administrator, and major network changes are additionally approved by the ISSO.

7.5.4 System Assurance

The procedures followed to validate the security posture of DCSNET can be found in Attachment I – DCSNET Certification Test Plan.

7.5.5 Unique Security Features

None.

7.5.6 Recovery Procedures

7.5.7 After Hours Processing

DCSNET equipment is designed and configured to operate 24x7.

7.5.8 System Start-Up

DCSNET equipment is designed and configured to operate 24x7.

7.5.9 Compliance-Monitoring Program

The procedures followed to validate the security posture of DCSNET can be found in Attachment I – DCSNET Certification Test Plan.

7.5.10 Non-Repudiation

7.5.11 Transaction Rollback

Not Applicable. DCSNET does not store data.

7.6 Auditing

7.6.1 Auditing Procedures

7.6.2 Notification Banner

7.6.3 User Accountability

7.6.4 Audit Protection

7.6.5 Audited Information

7.6.6 Audited Activities

7.6.7 Audit Review

7.6.8 Discrepancy Handling

7.6.9 System Verification and Testing

The procedures followed to validate the security posture of DCSNET can be found in Attachment I – DCSNET Certification Test Plan.

7.7 Marking and Labeling

7.7.1 System Hardware

7.7.2 Storage Media

N/A

7.7.3 Printout, Hardcopy

N/A

7.7.4 Internal Labeling

N/A

7.7.5 Exceptions

None.

7.8 Maintenance Procedures

7.8.1 General

7.8.2 Uncleared Personnel

7.8.3 Logs

7.8.4 Maintenance Software

7.8.5 Remote Diagnostics

7.9 Sanitization and Destruction

7.9.1 Hardware

DCSNET hardware is unclassified.

7.9.2 Data Storage Media

DCSNET does not use storage media.

7.10 Software Security Procedures

7.10.1 Procurement

Only approved, vendor-supplied software and firmware is used on DSCNET equipment.

7.10.2 Evaluation

A test bed consisting of several routers has been created for testing purposes. All new software loads and major changes to configurations are tested in the lab. This test bed simulates the live network using the same hardware and software. Changes are tested over the course of a week, if time permits, before being loaded onto the live systems.

7.10.3 Malicious Code/Virus Protection

7.10.4 Data and Software Integrity Procedures

DCSNET does not store data. Vendor-supplied software and firmware integrity is ensured by comparing hash signatures of procured software and firmware with vendor supplied hashes for that software and firmware.

7.11 Media Movement

N/A.

7.11.1 Media Introduction and Removal Procedures

N/A.

7.11.2 Data Copying, Reviewing, and Releasing Procedures

N/A.

7.12 Hardware Control

7.12.1 Transfer

7.12.2 Relocation

7.12.3 Release

7.12.4 Maintenance

7.12.5 Introduction of Hardware

7.13 Web Protocol and Distributed/Collaborative Computing

7.13.1 Web Server/Clients

N/A.

7.13.2 Mobile/Executable Code

N/A.

7.13.3 Collaborative Processes

N/A.

7.13.4 Distributed Processes

N/A.

7.14 Wireless Devices

DCSNET does not use or support the use of wireless devices.

7.15 PKI Use

DCSNET does not use PKI.

8.0 Security Awareness Program

8.1 Program Description

Security Awareness Training is provided by the Security Division and is required by all FBI employees.

8.2 Users Guides

9.0 Interconnection Security Agreement

Not Applicable.

10.0 Memoranda of Agreement

Not Applicable.

11.0 Availability

11.1 Restoration Procedures

Current system configurations are maintained in a management database. In the event of a corrupted or malfunctioning router, a new router can be configured and sent out within hours to replace the old one. All other DCSNET equipment is maintained by Sprint with a 4 hour on-site Service Level Agreement to replace an malfunctioning hardware.

11.2 Communications Back-up

Plans are being discussed to setup dial-up lines in the event of a primary circuit failure. Communications over this line would be encrypted to the same standards as the primary circuit. The dial-up circuits should fail-over automatically, keeping network availability high.

11.3 Power Back-up

Offices that don't have battery backups are being supplied with a UPS to power the router and any directly connected hardware (CSU/DSU, smartjack, etc.). It is the responsibility of each field office to maintain the UPS and be sure backup generator power is available in the event of an extended power outage.

11.4 Denial-of-Service Prevention

As there is no public connection to the DCSNET, and due to the vpn nature of the Sprint network, DOS attacks are not applicable. Even so, access-lists are applied to external interfaces to prevent any unauthorized traffic from affecting the router.

11.5 Priority Process Protection

Not Applicable.

12.0 Exceptions

Not Applicable.

13.0 Glossary of Terms

Attachment A – DCSNET Org Chart

[redacted]		Chief Technologist		[redacted]
		Electronics Engineer		
		Electronics Technician		
		Electronics Engineer		
		Electronics Technician		

b6
b7C

Attachment B – System Layouts

Attachment C – DCSNET System Block Diagram

[redacted]

b2
b7E

Attachment D – Equipment List

Nomenclature	Manufacturer	Model	Non-Volatile Memory	Serial Number	Location
Router	Cisco	2610XM	96MB Flash ROM	Jmx0725L54V	ERF
Router	Cisco	2610XM	96MB Flash ROM	Jmx0726L00T	Pittsburgh

FBI IT COOP Critical Systems by Branch / Office

The following table summarizes the FBI IT COOP Critical Systems List. It presents the number of critical systems by branch and their known recovery capabilities. All projects that were not designated Critical by Branch EADs (represented with capability = 0) were removed from this list. The details to support this summary table are presented in the tables on the following pages. The systems with sub-systems are listed in **boldface** with the sub-systems indented with grey fill-in. The sub-systems are not counted in the overall totals for each branch.

Branch / Office	RECOVERY CAPABILITY			Totals
	Recoverable in < 12 hrs	Not Recoverable in < 12 hrs	Recovery Capability Unknown	
Director's Office (DO) / Associate Deputy Director (ADD)	6	4	12	**22**
Chief Information Officer (CIO)	4	6	2	**12**
Criminal, Cyber, Response, & Services Branch (CCRSB)	3	3	1	**7**
Human Resources Branch (HRB)	0	0	1	**1**
Science & Technology Branch (STB)	3	10	40	**53**
National Security Branch (NSB)	7	8	12	**27**
Totals	**23**	**31**	**68**	**122**

Summary of Changes from 11/09/06 list to 12/05/06	
11/09 System Count	**152**
Systems Made into Sub-Systems	26
Systems Removed from List	4
12 / 05 System Count	**122**

For a detailed tracking of the changes made between the 11/09 list and the 12/05 list refer to the provided Change Control Log located in Appendix – A.

DATE: 06-05-2007
CLASSIFIED BY 65270 DMH/TAM/KSR/JB
REASON: 1.4 (g)
DECLASSIFY ON: 06-05-2032

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SYSTEMS BELONGING TO Science & Technology Branch (53)					RECOVERY CAPABILITY		
Line Item Class.	NAME	ACRONYM	DESCRIPTION	BRANCH	Recov. in < 12 hrs	Not Recov. in < 12 hrs	Capability Unknown
(S)	[redacted]						1 b1
(S)							b2 b7E
(U)	Digital Collection System 3000	DCS 3000	~~(S)~~ [DCS3000 application suite was developed to assist law enforcement agencies (LEAs) with collecting and processing data for court-ordered electronic surveillance (ELSUR) operations. LEAs dial into switches.]	STB		1	
~~(S)~~	~~(S)~~ [redacted]	~~(S)~~ [redacted]	~~(S)~~ [redacted]	STB			
(U)	[redacted]	[redacted]	~~(S)~~ [redacted]	STB		b2 b7E	
(U)	Digital Collection System Network	DCSNet	The Digital Collection Systems Network (DCSNET) is a transport mechanism for moving CALEA CDC and streamed CCC data from the service provider sources to the proper FBI Field Office destinations	STB			
(U)	[redacted]	[redacted]	[redacted]	STB			1
(U)	[redacted]	[redacted]	[redacted]	STB			1
(U)	[redacted]	[redacted]	[redacted]	STB			1

SYSTEMS BELONGING TO Science and Technology Branch (64)									
Line Item Class.	NAME	ACRONYM	BRANCH	SPONSORING ORGANIZATION	JEH Recoverable in < 12 hrs	CLK Recoverable in < 12 hrs	Other Locations Recoverable in < 12 hrs	Not Recoverable in < 12 hrs	Recovery Capability Unknown
(U)	**Digital Collection System 3000**	DCS 3000	Science and Technology	Operational Technology Division				1	
~~(S)~~	~~(S)~~ [redacted]	~~(S)~~ [redacted]	[redacted]	[redacted]				1	
(U)	[redacted]	[redacted]	[redacted]	[redacted]				1	
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]		[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					0
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]		[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]	[redacted]	[redacted]	[redacted]					1
(U)	[redacted]		[redacted]	[redacted]					1

b2
b7E

~~SECRET~~
(3)