Joint DoDIIS/Cryptologic SCI Information Systems Security Standards

11 April 2003
Revision 3

EXECUTIVE SUMMARY **I**

CHAPTER 1 - GENERAL INFORMATION **1**

1.1(U) BACKGROUND **1**
1.2 (U) POLICY **1**
1.3 (U) SCOPE AND APPLICABILITY **1**
1.4 (U) REFERENCES, ACRONYMS, AND DEFINITIONS **2**
1.5 (U) ROLES AND RESPONSIBILITIES **2**
1.5.1 (U) PRINCIPAL ACCREDITING AUTHORITY (PAA) 2
1.5.2 (U) DATA OWNER 3
1.5.3 (U) DESIGNATED ACCREDITING AUTHORITY (DAA) 3
1.5.4 (U) DAA REPRESENTATIVE (REP)/SERVICE CERTIFYING ORGANIZATION (SCO) 4
1.5.5 (U) NSA/CSS SENIOR INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (SISSPM) 5
1.5.6 (U) SERVICE CRYPTOLOGIC ELEMENT (SCE) INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM) 5
1.5.7 (U) COMMANDER/COMMANDING OFFICER (CO)/SENIOR INTELLIGENCE OFFICER (SIO) RESPONSIBILITY 6
1.5.8 (U) INFORMATION SYSTEMS SECURITY MANAGER (ISSM) 7
1.5.9 (U) INFORMATION SYSTEMS SECURITY OFFICER (ISSO) 8
1.5.10 (U) THE PROGRAM MANAGEMENT OFFICE (PMO)/PROGRAM MANAGER (PM) 9
1.5.11 (U) PRIVILEGED USERS (E.G., SYSTEM ADMINISTRATOR [SA]) 10
1.5.12 (U) GENERAL USERS 12
1.5.13 (U) PROHIBITED ACTIVITIES 12
1.6 (U) CONFIGURATION CONTROL BOARD (CCB) OVERSIGHT 13
1.7 (U) OTHER DOCUMENTATION SUPERSESSION 13

CHAPTER 2 - LIFE CYCLE SECURITY **14**

2.1 (U) PURPOSE **14**
2.2 (U) SCOPE **14**
2.3 (U) PROCEDURES **14**
2.3.1 (U) CONCEPTS DEVELOPMENT PHASE 14
2.3.1.1 (U) IS Security Design 15
2.3.1.2 (U) Statement of Work (SOW) Requirements 15
2.3.1.3 (U) Additional Documentation 15
2.3.2 (U) DESIGN PHASE 15
2.3.2.1 (U) Levels-of-Concern 15
2.3.2.2 (U) Protection Levels 16
2.3.2.2.1 (U) IS Protection Level Determinations 16
2.3.2.2.2 (U) Security Documentation (SSP/SSAA) Requirements 16
2.3.3 (U) DEVELOPMENT PHASE 16
2.3.4 (U) TEST, CERTIFICATION AND ACCREDITATION PHASE 17

2.3.4.1 (U) Time Line for Certification Activities 17
2.3.5 (U) DEPLOYMENT AND OPERATIONS PHASE 17
FIGURE: 2.1 – EXAMPLE PROCESS FOR PL2 DODIIS IMA AFTER APPROVAL TO FIELD. 18
2.3.6 (U) CONTINGENCY PLANNING 18
2.3.7 (U) RECERTIFICATION/REACCREDITATION PHASE 19
2.3.8 (U) DISPOSAL PHASE 19

CHAPTER 3 - SIGNALS INTELLIGENCE (SIGINT) SYSTEMS ACCREDITATION PROCESS AND PROCEDURES 20

3.1 (U) PURPOSE 20
3.2 (U) SCOPE 20
3.3 (U) DISCUSSION 20
3.3.1 (U) ACCREDITATION 20
3.3.2 (U//FOUO) NISCAP 20
3.3.3 (U) CONFIGURATION MANAGEMENT 20
3.4 (U) NISCAP FLOW 21
FIGURE 3.1 (U) NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE INFORMATION SYSTEM CERTIFICATION AND ACCREDITATION PROCESS 21
3.4.1 (U) GENERAL ACCREDITATION APPROVALS 21
3.4.2 (U) INTERIM APPROVAL TO OPERATE (IATO) 21
3.4.3 (U) REACCREDITATION 22
3.4.4 (U) RESCINDING ACCREDITATIONS 22
3.4.5 (U) ACCREDITATION THREE-YEAR ANNIVERSARY REVIEW 22
3.4.6 (U) INFORMATION SYSTEMS (IS) EXEMPTED FROM ACCREDITATION UNDER NISCAP 22
3.4.7 (U) TEMPEST 23
3.5 (U) REQUESTS FOR ACCREDITATION 23
FIGURE 3.2 ACCREDITATION PROCESS AT SCE SITES/UNITS 23
3.5.1 (U) ACCREDITATION REQUESTS INITIATED AT THE UNIT LEVEL FOR PL 1 AND PL 2 ISS WITH ONLY BASIC/MEDIUM INTEGRITY LEVEL OF CONCERN (ILOC)/AVAILABILITY LEVEL OF CONCERN (ALOC) 23
3.5.1.1 (U) ISSM review of PL 1 and PL 2 Documentation 24
3.5.2 (U) ACCREDITATION REQUESTS INITIATED AT THE UNIT LEVEL FOR PL 3, PL 4, PL 5 24
3.5.3 (U) DOWNWARD-DIRECTED ACCREDITATION FROM PROGRAM MANAGEMENT/PROJECT OFFICES 24
3.5.4 (U) ACCREDITATION REQUESTS INITIATED AT A SINGLE-SERVICE SITE 25
3.5.5 (U) SUBMISSION OF THE SSP AND NISCAP DOCUMENTATION 25
3.5.6 (U) FORMAT AND CONTENT 25

CHAPTER 4 - DODIIS SITE-BASED ACCREDITATION AND SYSTEM CERTIFICATION 26

4.1 (U) PURPOSE 26
4.2 (U) SCOPE 26
4.3 (U) SYSTEM CERTIFICATION AND ACCREDITATION PROCEDURES: 26
4.3.1 (U) SYSTEM CERTIFICATION AND ACCREDITATION COMPLIANCE 26
4.3.2 (U) SYSTEM CERTIFICATION AND ACCREDITATION PROCESS 27
4.3.2.1 (U) Phase 1 27
4.3.2.2 (U) Phase 2 27
4.3.2.3 (U) Phase 3 27
4.3.2.4 (U) Phase 4 27
4.3.3 (U) DODIIS CERTIFICATION AND ACCREDITATION FOR EXERCISE OR EXPERIMENT SCENARIOS 27
4.3.3.1 (U) Simulated Network Connectivity 27

4.3.3.2 (U) JWICS Connection 28
4.3.3.3 (U) Exercise Use of Multiple Operational Network Connectivity 28
4.4 (U) SITE-BASED ACCREDITATION METHODOLOGY 28
4.4.1 (U) SITE-BASED ACCREDITATION METHODOLOGY COMPLIANCE 28
4.4.2 (U) THE SITE-BASED ACCREDITATION PROCESS 28
4.4.2.1 (U) Initial Site Visit (Initial Site Certification Visit) 28
4.4.2.2 (U) Site Evaluation Visit 29
4.4.2.3 (U) Site Compliance Visit (Vulnerability Assessment and Compliance Verification) 29
4.5 (U) CONTRACTOR ACCREDITATION 29
4.6 (U) ACCREDITATION REVIEW 29
4.6.1 (U) GUEST SYSTEMS IN A SCIF 29
4.6.1.2 (U) SCI Systems with Certification 29
4.6.1.3 (U) SCI Systems without Certification 30
4.6.1.4 (U) Unclassified or Collateral Systems 30
4.7 (U) MINIMUM SECURITY REQUIREMENTS 30
4.7.1 (U) SSAA CONTENT CLASSIFICATION 30
4.8 (U) CERTIFICATION (IATO) AND ACCREDITATION (ATO) AUTHORITY 30
4.8.1 (U) CERTIFICATION AND ACCREDITATION AUTHORITY FOR PROTECTION LEVEL 1 AND 2 31
4.8.2 (U) CERTIFICATION AND ACCREDITATION AUTHORITY FOR PROTECTION LEVEL 1, 2 AND 3 31
4.8.3 (U) CERTIFICATION AUTHORITY FOR PROTECTION LEVEL 4 AND 5 31
4.8.4 (U) CERTIFICATION AUTHORITY FOR DODIIS SITE BASELINES 31
4.8.5 (U) ACCREDITATION AUTHORITY FOR PROTECTION LEVEL 4, 5 AND DODIIS SITE BASELINES 31
4.8.6 (U) INTERIM APPROVALS TO TEST (IATT) 31
FIGURE 4-1: IATO/ATO AUTHORITY 32

CHAPTER 5 - TEMPEST 33

5.1 (U) PURPOSE 33
5.2 (U) SCOPE 33
5.3 (U) DEFINITIONS 33
5.4 (U) TEMPEST COMPLIANCE 34
5.5 (U) ACCREDITATION 34
5.5.1 (U) TEMPEST COUNTERMEASURES REVIEW 34
5.5.2 (U) GENERAL DOCUMENTATION 34
5.5.3 (U) TEMPEST/ISD ACCREDITATION 34
5.6 (U) TEMPEST INSTALLATION REQUIREMENTS: 34

CHAPTER 6 - MINIMUM SECURITY REQUIREMENTS FOR USERS 36

6.1 (U) PURPOSE 36
6.2 (U) SCOPE 36
6.3 (U) MINIMUM SECURITY REQUIREMENTS 36
6.3.1 (U) IDENTIFICATION AND AUTHENTICATION REQUIREMENTS 36
6.3.2 (U) PASSWORD REQUIREMENTS 36
6.3.3 (U) IS WARNING BANNER 37
6.3.4 (U) CONFIGURATION MANAGEMENT REQUIREMENTS 38
6.3.4.1 (U) Authorized Software 38
6.3.4.2 (U) Unauthorized Software 38
6.3.5 (U) MALICIOUS CODE DETECTION 39
6.3.6 (U) MALICIOUS CODE PREVENTION 39

6.3.7 (U) REMOVABLE INFORMATION STORAGE MEDIA 39
6.3.7.1 (U) Label Placement 40
6.3.7.2 (U) Data Descriptor Label 40
6.3.7.3 (U) Classification Markings 40
6.3.7.4 (U) Control and Accounting of Media 40
6.3.7.4.1 (U) Information Storage Media Control 40
6.3.7.4.2 (U) Inspections 40
6.3.7.4.3 (U) Control Procedures 40
6.3.7.4.4 (U) Other Categories of Storage Media 41
6.3.8 (U) HARDWARE LABELING REQUIREMENTS 41
6.3.9 (U) SECURITY TRAINING REQUIREMENTS 41
6.3.9.1 (U) Security Awareness and Training Program 41
6.3.9.1.1 (U) Awareness Level 41
6.3.9.1.2 (U) Performance Level 42
6.3.9.1.3 (U) General Users training 42
6.3.10 (U) Destruction of Media 42
6.3.11 (U) Information Transfer and Accounting Procedures 42

CHAPTER 7 - SECURITY GUIDELINES FOR THE PRIVILEGED USER 43

7.1 (U) PURPOSE 43
7.2 (U) SCOPE 43
7.3 (U) SECURITY TRAINING 43
7.3.1 (U) PRIVILEGED USER TRAINING 43
7.3.2 (U) SECURITY AWARENESS AND TRAINING PROGRAM 44
7.3.2.1 (U) Awareness Level 44
7.3.3.2 (U) Performance Level 44
7.4 (U) LEAST PRIVILEGE IMPLEMENTATION 44
7.5 (U) SCI SYSTEM SECURITY PROCEDURES 44
7.5.1 (U) IDENTIFICATION AND AUTHENTICATION REQUIREMENTS 44
7.5.1.1 (U) Documenting USERIDs and Passwords 44
7.5.1.2. (U) USERID and Password Issuing Authority and Accountability 45
7.5.1.3 (U) Supervisor Authorization 45
7.5.1.4 (U) Access Requirements Validation 45
7.5.1.5 (U) Account Management 45
7.5.1.6 (U) Tactical/Deployable Use of group accounts 45
7.5.2 (U) SYSTEM ACCESS AND REMOVAL PROCEDURES 46
7.5.3 (U) AUDIT TRAIL REQUIREMENTS 46
7.5.3.1 (U) Automated Audit Trail Information Requirements 46
7.5.3.2 (U) Manual Audit Trail Implementation 47
7.5.3.3 (U) Products of Audit Trail Information 47
7.5.3.4 (U) Audit Trail Checks and Reviews 48
7.5.3.5 (U) Audit Trail Records Retention 48
7.5.3.6 (U) Tactical/Deployable Audit Process Requirements 48
7.5.3.6.1 (U) Tactical/Deployable Audit log requirements 48
7.5.4 (U) AUTOMATIC LOG-OUT REQUIREMENTS 48
7.5.5 (U) LIMITED ACCESS ATTEMPTS 48
7.5.6 (U) USE OF WINDOWS SCREEN LOCKS 49
7.5.6.1 (U) Tactical/Deployable Protection for Information against unattended operation 49
7.5.7 (U) TESTING, STRAINING, AND HACKING 49
7.5.8 (U) WARNING BANNERS 49

7.5.9 (U) NETWORK MONITORING 49
7.5.9.1 (U) Maintenance Monitoring 49
7.5.9.2 (U) Targeted Monitoring 50

CHAPTER 8 - INFORMATION SYSTEMS (IS) INCIDENT REPORTING 51

8.1 (U) PURPOSE 51
8.2 (U) SCOPE 51
8.3 (U) PROCEDURES 51
8.3.1 (U) REPORTING PROCESS 51
8.3.2 (U) TYPES OF IS INCIDENTS AND REPORTS 51
8.3.3 (U) REPORTING INCIDENTS 52
8.3.4 (U) REPORT FORMAT AND CONTENT 53
FIGURE 8.1 (U) SAMPLE INCIDENT REPORT MESSAGE 54
8.3.5 (U) FOLLOW-ON ACTION 54

CHAPTER 9 - INFORMATION SYSTEM (IS) MONITORING ACTIVITIES 55

9.1 (U) PURPOSE 55
9.2 (U) SCOPE 55
9.3 (U) PROCEDURES 55
9.3.1 (U) IS WARNING BANNER 55
FIGURE 9.1. (U) INFORMATION SYSTEM WARNING BANNER. 56
9.3.2 (U) WARNING LABELS 56
FIGURE 9.2. (U) WARNING LABEL. 56
9.3.3 (U) ACTION TO BE TAKEN BEFORE MONITORING 56
9.3.4 (U) REVIEW SYSTEM SPECIFIC SECURITY FEATURES 57
TABLE 9.1. (U) RECOMMENDED INCIDENT RESPONSE ACTIONS 57
TABLE 9.2. (U) SAMPLE MONITORING INVESTIGATION QUESTIONS 57

CHAPTER 10 - MALICIOUS CODE PREVENTION 59

10.1 (U) PURPOSE 59
10.2 (U) SCOPE 59
10.3 (U) DEFINITIONS 59
10.3.1 (U) MALICIOUS CODE 59
10.3.2 (U) MOBILE CODE 59
10.3.3 (U) MALICIOUS MOBILE CODE 59
10.3.4 (U) MOBILE CODE TECHNOLOGIES 60
10.3.4.1 (U) Red Mobile Code 60
10.3.4.2 (U) Yellow Mobile Code 60
10.3.4.3 (U) Green Mobile Code 61
10.3.4.4 (U) Emerging Mobile Code Technologies 61
10.3.4.5 (U) Exempt technologies 61
10.3.5 (U) TRUSTED SOURCE 61
10.3.6 (U) SCREENING 62
10.4 (U) PROCEDURES 62
10.4.1 (U) PREVENTIVE PROCEDURES 62
10.4.2 (U) MALICIOUS CODE DETECTION 62

10.5 (U) MALICIOUS CODE SECURITY REQUIREMENTS **63**
10.5.1 (U) PREVENTATIVE STEPS TO BE TAKEN 63

CHAPTER 11 - SOFTWARE **64**

11.1 (U) PURPOSE **64**
11.2 (U) DEFINITION **64**
11.3 (U) SCOPE **64**
11.4 (U) PROCEDURES FOR SOFTWARE AUTHORIZATION **64**
11.5 (U) LOW RISK SOFTWARE **64**
11.6 (U) HIGH RISK SOFTWARE **64**
11.6.1 (U) PUBLIC DOMAIN SOFTWARE 65
11.6.2 (U) DEMONSTRATION SOFTWARE AND MEDIA 65
11.6.3 (U) EMBEDDED SOFTWARE 65
11.6.4 (U) UNAUTHORIZED SOFTWARE 65
11.6.5 (U) IA SOFTWARE AND SECURITY TOOLS 65

CHAPTER 12 - INFORMATION STORAGE MEDIA **66**

12.1 (U) PURPOSE **66**
12.2 (U) SCOPE **66**
12.3 (U) CONTROL AND ACCOUNTING PROCEDURES **66**
12.3.1 (U) INFORMATION STORAGE MEDIA CONTROL 66
12.3.1.1 (U) Inspections 66
12.3.1.2 (U) Control Procedures 66
12.3.1.3 (U) Other Categories of Storage Media 66
12.3.2 (U) AUDITS AND REPORTS 67
12.3.3 (U) DESTRUCTION OF MEDIA 67
12.4 (U) MEDIA LABELING PROCEDURES **67**
12.4.1 (U) INFORMATION STORAGE MEDIA 67
FIGURE 12.1 – SF 700 SERIES LABELS 68
12.4.1.1 (U) Label Placement 68
12.4.1.2 (U) Data Descriptor Label 68
12.4.2 (U) Tactical/Deployable Labeling media and hardware components 69
12.4.3 (U) CLASSIFICATION MARKINGS 69

CHAPTER 13 - INFORMATION SYSTEMS (IS) MAINTENANCE PROCEDURES **70**

13.1 (U) PURPOSE **70**
13.2 (U) SCOPE **70**
13.3 (U) PROCEDURES **70**
13.3.1 (U) MAINTENANCE PERSONNEL 70
13.3.1.1 (U) Maintenance by Cleared Personnel 70
13.3.1.2 (U) Maintenance by Uncleared (or Lower-Cleared) Personnel 70
13.3.2 (U) GENERAL MAINTENANCE REQUIREMENTS 71
13.3.2.1 (U) Maintenance Log 71
13.3.2.2 (U) Location of Maintenance 71
13.3.2.3 (U) Removal of Systems/Components 71
13.3.2.4 (U) Use of Network Analyzers 71

13.3.2.5 (U) Use of Diagnostics 71
13.3.2.6 (U) Introduction of Maintenance Equipment into a SCIF 71
13.3.3 (U) MAINTENANCE AND SYSTEM SECURITY 72
13.3.4 (U) REMOTE MAINTENANCE REQUIREMENTS/CONSIDERATIONS 72
13.3.4.1 (U) Maintenance Performed with the same Level of Security 72
13.3.4.2 (U) Maintenance Performed with a different Level of Security 72
13.3.4.3 (U) Initiating and Terminating Remote Access 72
13.3.4.4 (U) Keystroke Monitoring Requirements 72
13.3.5 (U) LIFE CYCLE MAINTENANCE 73

CHAPTER 14 – DIGITAL AND MULTI-FUNCTION DEVICES (COPY/PRINT/SCAN/FAX) 74

14.1 (U) PURPOSE 74
14.3 (U) POLICY 74
14.4 (U) PROCEDURES 75
14.4.1 (U) FAX CAPABILITIES 76
14.5 (U) RESPONSIBILITIES 76
14.5.1 (U) THE DAA REPRESENTATIVE SHALL: 76
14.5.2 (U) ISSOS AND/OR INFORMATION SYSTEMS SECURITY MANAGERS SHALL: 76
14.5.3 (U) USERS SHALL: 76

CHAPTER 15 - PORTABLE ELECTRONIC DEVICES 77

15.1 (U) PURPOSE 77
15.3 (U) RISK 77
15.3.1 (U) CLASSIFIED INFORMATION 77
15.4 (U) PROCEDURES 77
15.4.1 (U) APPROVAL REQUIREMENTS 77
15.4.1.1 (U) Personal PEDs 78
15.4.1.2 (U) Government Owned PEDs 78
15.4.1.3 (U) Contractor Business Owned PEDs 78
15.4.2 (U) HANDLING PROCEDURES 78
15.4.2.1 (U) Standard Operating Procedure (SOP) Development 79
15.4.2.2 (U) SOP Approval 79

CHAPTER 16 - SECURITY PROCEDURES FOR INFORMATION SYSTEMS (IS) AND FACSIMILE (FAX) USE OF THE PUBLIC TELEPHONE NETWORK 80

16.1 (U) PURPOSE 80
16.2 (U) SCOPE 80
16.3 (U) PROCEDURES 80
16.3.1 (U) FAX CONNECTIVITY 80
16.3.1.1 (U) FAX Approval 80
16.3.1.1.1 (U) Unclassified FAX. 81
16.3.1.1.2 (U) Classified FAX 81
16.3.1.1.3 (U) Non-Standard Secure Fax 81
16.3.1.1.4 (U) Procedures 82
16.3.1.1.5 (U) FAX Accreditation 83
16.3.2 (U) COMPUTER-FAX/MODEM CONNECTIVITY 83

16.3.2.1 (U) Unclassified Computer-FAX/Modem Accreditation Approval 83
16.3.2.2 (U) Physical Disconnect of Unclassified Computer-FAX/Modems 83
16.3.3 (U) COMPUTER-MODEM CONNECTIVITY 83
16.3.3.1 (U) Unclassified Computer-Modem Connectivity 83
16.3.3.1.1 (U) ISP Connectivity 83
16.3.3.1.2 (U) IS to IS Connectivity 83
16.3.3.2 (U) Classified Computer-Modem Connectivity 84
16.3.3.3 (U) Classified Computer-STU-III/STE Data Port Connectivity 84

CHAPTER 17 - INTERCONNECTING INFORMATION SYSTEMS 86

17.1 (U) PURPOSE 86
17.2 (U) SCOPE 86
17.3 (U) DISCUSSION 86
17.3.1 (U) INTERCONNECTED INFORMATION SYSTEMS 86
17.3.2 (U) INTER-DOMAIN CONNECTIONS 86
17.3.3 (U) CONTROLLED INTERFACE 87
17.3.3.1 (U) One-Way Connections 87
17.3.3.1.1 (U) Equal Classification Connections 87
17.3.3.1.2 (U) Low-to-High Connections 87
17.3.3.1.3 (U) High-to-Low Connections 87
17.3.3.1.4 (U) Other Unequal Classification Level Connections 87
17.3.3.2 (U) Dual-Direction Connections 88
17.3.3.3 (U) Multi-Domain Connections 88
17.3.4 (U) REVIEW PROCEDURES 88
17.3.4.1 (U) Reliable Human Review 88
17.3.4.2 (U) Automated Review 88
17.3.5 (U) FOREIGN NATIONAL ACCESS TO SYSTEMS PROCESSING CLASSIFIED INFORMATION 88

CHAPTER 18 - INFORMATION TRANSFER AND ACCOUNTING PROCEDURES 90

18.1 (U) PURPOSE 90
18.2 (U) SCOPE 90
18.3 (U) PROCEDURES 90
18.3.1 (U) RELIABLE HUMAN REVIEW OF DATA 90
18.3.2 (U) MEDIA TRANSFERS IN/OUT OF AN ORGANIZATION 91
18.3.3 (U) DISPOSITION OF EXCESS OR OBSOLETE COTS SOFTWARE 91
18.3.4 (U) HIGH-TO-LOW DATA TRANSFER BY MEDIA 91
18.3.4.1 (U) PL-3 and Below Functionality 92
18.3.4.2 (U) PL-4 and Above Functionality 92
18.3.5 (U) LOW-TO-HIGH DATA TRANSFER BY MEDIA 92
18.3.6 (U) DEMONSTRATION SOFTWARE 93

CHAPTER 19 - MULTI-POSITION SWITCHES 94

19.1 (U) PURPOSE 94
19.2 (U) SCOPE 94
19.3 (U) POLICY 94
19.4 (U) RESPONSIBILITIES 94

19.4.1 (U) DAA REP 94
19.4.2 (U) ISSM 95
19.4.3 (U) ISSO/SYSTEM ADMINISTRATOR 95
19.4.4 (U) USER 95
19.5 (U) IS REQUIREMENTS **95**
19.6 (U) PROCEDURES FOR LOGON/SWITCHING BETWEEN SYSTEMS **96**
19.6 1 (U) LOGGING ON TO SYSTEMS 96
19.6.2 (U) SWITCHING BETWEEN SYSTEMS 97
19.7 (U) KVM SWITCH USER AGREEMENT **97**
FIGURE 19.1 (U) KVM SWITCH USER AGREEMENT FORM. 98

CHAPTER 20 – COLLABORATIVE COMPUTING **99**

20.1 (U) PURPOSE **99**
20.2 (U) SCOPE **99**
20.3 (U) IMPLEMENTATION PROCEDURES **99**
20.3.1 (U) COLLABORATIVE COMPUTING ACTIVATION 99
20.3.2 (U) VIDEO CAMERAS/MICROPHONES CONNECTED TO SCI INFORMATION SYSTEMS 100
20.3.3 (U) VIDEO CAMERAS/MICROPHONES CONNECTED TO COLLATERAL/UNCLASSIFIED INFORMATION SYSTEMS 100
20.3.4 (U) COLLABORATIVE COMPUTING APPROVAL 100
20.3.5 (U) RESPONSIBILITIES 100

CHAPTER 21 - CLEARING, SANITIZING, AND RELEASING COMPUTER COMPONENTS **102**

21.1 (U) PURPOSE **102**
21.2 (U) SCOPE **102**
21.3 (U) RESPONSIBILITIES **102**
21.4 (U) REVIEW OF TERMS 102
21.5 (U) PROCEDURES **103**
21.5.1 (U) OVERWRITING MEDIA 103
21.5.2 (U) DEGAUSSING MEDIA 103
21.5.2.1 Types of Degausser 103
21.5.2.2 (U) Degausser Requirements 104
21.5.2.3 (U) Use of a Degausser 104
21.5.3 (U) SANITIZING MEDIA 104
TABLE 21.1. (U) SANITIZING DATA STORAGE MEDIA 104
TABLE 21.2. (U) SANITIZING SYSTEM COMPONENTS 105
21.5.4 (U) DESTROYING MEDIA 106
21.5.4.1 (U) Expendable Item Destruction 106
21.5.4.1.1 (U) Shipping Instructions 106
21.5.4.2 (U) Destruction of Hard Disks 107
21.5.4.2.1 (U) Shipping Instructions 107
21.5.4.3 (U) Destruction of Disk Packs 108
21.5.4.4 (U) Optical Storage Media Destruction 108
21.5.5 (U) MALFUNCTIONING MEDIA 108
21.5.6 (U) RELEASE OF MEMORY COMPONENTS AND BOARDS 108
21.5.6.1 (U) Volatile Memory Components 109
21.5.6.2 (U) Non-volatile Memory Components 109
21.5.6.3 (U) Other Non-volatile Media 109

21.5.6.3.1 (U) Visual Displays 109
21.5.6.3.2 (U) Printer Platens and Ribbons 109
21.5.6.3.3 (U) Laser Printer Drums, Belts, and Cartridges 109
21.5.7 (U) CLEARING SYSTEMS FOR PERIODS PROCESSING 110
21.5.8 (U) RELEASE OF SYSTEMS AND COMPONENTS 110
21.5.8.1 (U) DOCUMENTING IS RELEASE OR DISPOSAL 111
FIGURE 21.1. (U) SAMPLE NSACSS FORM G6522 111

CHAPTER 22 - INFORMATION SYSTEMS (IS) AND NETWORK SECURITY SELF-INSPECTION AID 112

22.1 (U) PURPOSE 112
22.2 (U) SCOPE 112
22.3 (U) APPLICABILITY 112
22.4 (U) PROCEDURES 112
TABLE 22.1 (U) IS AND NETWORK SECURITY SELF-INSPECTION CHECKLIST 113

APPENDIX A - REFERENCES 123

PUBLIC LAWS 123
EXECUTIVE ORDERS 123
NATIONAL PUBLICATIONS 123
DEPARTMENT OF DEFENSE (DoD) PUBLICATIONS 124
DEFENSE INTELLIGENCE AGENCY (DIA) PUBLICATIONS 124
NATIONAL SECURITY AGENCY (NSA)/CENTRAL SECURITY SERVICE (CSS) PUBLICATIONS 124

APPENDIX B – ACRONYMS & ABBREVIATIONS 126

APPENDIX C – GLOSSARY OF TERMS 131

APPENDIX D - SUMMARY OF CHANGES 146

EXECUTIVE SUMMARY

(U) The policy of the U.S. Government is that all classified information must be appropriately safeguarded to assure the confidentiality, integrity, and availability of that information. This document provides procedural guidance for the protection, use, management, and dissemination of Sensitive Compartmented Information (SCI), and is applicable to the Department of Defense (DoD) to include DoD components and Government contractors who process SCI. The combination of security safeguards and procedures used for Information Systems (IS) shall assure compliance with DoD 5105.21-M-1, Director, Central Intelligence Directive 6/3 (DCID 6/3), National Security Agency/Central Security Service (NSA/CSS) Manual 130-1 and the Defense Intelligence Agency Manual (DIAM 50-4). The Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS) is a technical supplement to both the NSA/CSS Manual 130-1 and DIAM 50-4.

(U) The prime purpose of this document is to provide IS security implementation guidance relative to the management of SCI and the automated infrastructure used to process this information at the organizational level.

(U) Nothing in this document shall be construed to countermand or waive provisions of any Executive Order, National Policy, DoD Directive, or other provisions of regulatory policies or laws which are beyond the scope of authority of the Directors of the Defense Intelligence Agency (DIA) and the National Security Agency/Central Security Service (NSA/CSS).

CHAPTER 1 - GENERAL INFORMATION

1.1(U) BACKGROUND

The DIA DoDIIS Information Assurance (IA) Program includes the Air Force, Army, Navy, and National Imagery and Mapping Agency (NIMA) Service Certification Organizations (SCO). The NSA/CSS Cryptologic Information Assurance (IA) Program includes the Air Force, Army, and Navy Service Cryptologic Elements (SCE). Together, they identified a requirement to standardize security procedures used in the management of Sensitive Compartmented Information (SCI) systems and the information they process. SCI is defined as information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. It was also determined that by standardizing procedural guidelines, it would significantly improve support to the increasingly interconnected customer base of the Joint Services. This document describes the protection philosophy and functional procedures essential in the implementation of an effective IA Program. Further, it provides implementation guidelines and procedures applicable to the protection, use, management, and dissemination of SCI; assigns responsibilities; and establishes procedures for the development, management, and operations of systems and networks used for processing SCI. The primary purpose of this supplemental guidance is to address day-to-day IS security (ISS) issues and provide support to those responsible for managing SCI and the automated infrastructure used to process this information at the organizational level.

1.2 (U) POLICY

U.S. Government policy requires all classified information be appropriately safeguarded to ensure the confidentiality, integrity, and availability of the information. Safeguards will be applied such that information is accessed only by authorized persons and processes, is used only for its authorized purpose, retains its content integrity, is available to satisfy mission requirements, and is marked and labeled as required. SCI created, stored, processed, or transmitted in or over Information Systems (ISs) covered by DCI policy and supplementing directives shall be properly managed and protected throughout all phases of a system's life cycle. The combination of security safeguards and procedures shall assure that the system and users are in compliance with DCID 6/3, DoD 5105.21-M-1, NSA/CSS Manual 130-1, DIAM 50-4, and this supplement (e.g., JDCSISSS). This document shall not be construed to countermand or waive provisions of any Executive Order, National Policy, DoD Directive, or other provisions of regulatory policies or laws, which are beyond the scope of authority of the Directors of the DIA and the NSA/CSS. Any perceived contradictions with higher-level policy should be forwarded to the appropriate Designated Accrediting Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) for resolution.

1.3 (U) SCOPE AND APPLICABILITY

This document contains procedures and identifies standards that shall be applied to all systems processing SCI under the cognizance of the DoD. This includes the following:

- Office of the Secretary of Defense (OSD)
- the Chairman of the Joint Chiefs of Staff
- the Joint Staff
- the United, Joint Commands and Task Forces

- the Defense Agencies and Field Activities
- the Military Departments (including their National Guard and Reserve components)
- NSA/CSS and its Service Cryptologic Elements
- NIMA
- the Inspector General of the DoD
- and Government contractors supporting DoD who process SCI.

This includes systems that are: airborne, mobile, afloat, in-garrison, tactical, mission, administrative, embedded, portable, Government purchased, Government leased, or on loan from other Government sources, and Contractor purchased and leased.

Contained also within this document is a collective set of procedures and protection mechanisms for ISs and networks used in SCI processing that must be enforced throughout all phases of the IS life-cycle, to include:

- Concept Development
- Design
- Development
- Deployment
- Operations
- Recertification
- Disposal

1.4 (U) REFERENCES, ACRONYMS, AND DEFINITIONS

Appendix A provides a comprehensive list of national, department, and agency publications that are used in conjunction with this document and augments these reference sources. The acronyms used in this document are contained in part 1 of Appendix B. The terminology extracted from various IS related documents are included as part 2 of Appendix B.

1.5 (U) ROLES AND RESPONSIBILITIES

The roles and responsibilities of the personnel involved with IS security are summarized in the paragraphs below. Personnel in the roles defined below must attend training and certification as directed by DoD and meet DCID 6/3 prerequisites. Reference appendix C for list of PAAs and DAAs.

1.5.1 (U) Principal Accrediting Authority (PAA)

The PAA has ultimate security responsibility for his/her organization. This responsibility includes IA program oversight, development, and implementation. In general, much of this person's operational authority is delegated to DAAs. The PAA shall:

- Be a U.S. citizen;
- Be an employee of the United States Government; and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

- Responsibilities of the PAA shall include:
- Establish a department or agency IA Security Program.
- Appoint DAAs.
- Approve or disapprove further delegation of the DAA's authority.
- Ensure that individuals knowledgeable in all areas of security support the DAA such that a technically correct assessment of the security characteristics of new ISs can be formalized.
- Ensure the implementation of the requirements set forth in U.S. Government IS security policy.
- Ensure accountability for the protection of the information under his/her purview.
- Ensure availability of security education, training, and awareness, to ensure consistency and reciprocity.
- Establish a compliance and oversight mechanism to validate the consistent implementation of IS security policy.
- When justified, approve the operation of system(s) that do not meet the requirements specified in DoD and Intelligence Community (IC) IS security documents. However, such approval shall be in writing, and the PAA granting such approval shall also document, in writing, his/her responsibility for the resulting residual risk(s) and inform other PAAs responsible for systems interconnected to this system.
- Ensure that security is incorporated as an element of the IS life-cycle process.

1.5.2 (U) Data Owner

Responsibilities of the Data Owner shall include, but are not limited to:

- Provide guidance to the PAA/DAA concerning:
- The sensitivity of information under the Data Owner's purview;
- The PAA/DAA's decision regarding the Levels-of-Concern for confidentiality, integrity, and availability; and
- Specific requirements for managing the owner's data (e.g., incident response, information contamination to other systems/media, and unique audit requirements).
- Determine whether foreign nationals may access information systems accredited under this manual. Access must be consistent with DCIDs 6/6, 5/6 and 6/3.

1.5.3 (U) Designated Accrediting Authority (DAA)

The DAA shall:

- Be a U.S. citizen;
- Be an employee of the United States Government; and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

Responsibilities of the DAA shall include, but are not limited to:

- Ensure each system is properly accredited/certified based on system environment, sensitivity levels and security safeguards.

- Issue written accreditation/certification statements.
- Ensure records are maintained for all IS accreditations/certifications under his/her purview to include use of automated information assurance tools.
- Ensure all of the appropriate roles and responsibilities outlined in this directive are accomplished for each IS.
- Ensure that operational information systems security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.
- Ensure that a security education, training, and awareness program is in place.
- Ensure that security is incorporated as an element of the life-cycle process.
- Ensure that the DAA Rep/ SCO members are trained and certified to properly perform their responsibilities.
- Provide written notification to the cognizant PAA and Data Owner prior to granting any foreign national access to the system.
- Ensure that organizations plan, budget, allocate, and spend adequate resources in support of IS security.
- Ensure consideration and acknowledgement of Counter-Intelligence activities during the C&A process.
- Report security-related events to affected parties (i.e., interconnected systems), data owners, and all involved PAAs.

1.5.4 (U) DAA Representative (Rep)/Service Certifying Organization (SCO)

- The DAA Rep(s)/SCO members shall be U.S. citizens and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

Responsibilities of the DAA Rep/SCO, under the direction of the DAA, shall include:

- Develop and oversee operational information systems security implementation policy and guidelines.
- Ensure that security testing and evaluation is completed and documented.
- Advise the DAA on the use of specific security mechanisms.
- Maintain appropriate system accreditation documentation.
- Oversee and periodically review system security to accommodate possible changes that may have taken place.
- Advise the Information Systems Security Managers (ISSMs) and Information System Security Officers (ISSOs) concerning the levels of concern for confidentiality, integrity, and availability for the data on a system.
- Evaluate threats and vulnerabilities to ascertain the need for additional safeguards.
- Ensure that a record is maintained of all security-related vulnerabilities and ensure serious or unresolved violations are reported to the DAA.

- Ensure that certification is accomplished for each IS.
- Evaluate certification documentation and provide written recommendations for accreditation to the DAA.
- Ensure all ISSMs and ISSOs receive technical and security training to carry out their duties.
- Assess changes in the system, its environment, and operational need that could affect the accreditation.

1.5.5 (U) NSA/CSS Senior Information Systems Security Program Manager (SISSPM)

- The SISSPM shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

The SISSPM responsibilities shall include but are not limited to the following:

- Develop metrics, measuring and reporting progress on improving ISS in operational systems and networks.
- Establish and maintain career development and training for ISS personnel under their purview.
- Serve as the operational representative to the NSA/CSS Information System Security Incident Board (NISSIB).
- Represent the operational ISS view to the Operational Information Systems Security Steering Group.
- Direct Field, SCE and regional ISSPMs in actions related to the NSA/CSS Operational IS Security Program.
- Assist the NISIRT in managing ISS incidents and in implementing fixes to identified vulnerabilities in operational ISs.
- Promote general operational information systems security awareness.
- Provide technical and policy guidance to ISS Security personnel.
- Provide a forum for information exchange on computer security issues with the Information Systems Security Managers.

1.5.6 (U) Service Cryptologic Element (SCE) Information Systems Security Program Manager (ISSPM)

- The SCE ISSPM shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

The SCE ISSPM responsibilities include:

- Act as liISon on matters concerning IS and Network security to the NSA/CSS Senior Information Systems Security Program Manager (SISSPM) and to the appropriate military headquarters.
- Ensure the accreditation of all SCE ISs.

- Review all certification/accreditation support documentation for proof of adequate IS and Network security procedures and, based upon the review, recommend approval or disapproval to the appropriate DAA.
- Forward reviewed certification/System Security Plan (SSP) for ISs to the NSA/CSS SISSPM, as required.
- Grant interim approval-to-operate and formal accreditation of ISs as authorized by NSA/CSS DAA.
- Review requests to bypass, strain, or test security mechanisms, or conduct network monitoring or keystroke monitoring and obtaining approval/disapproval for SCI requests from the NSA/CSS SISSPM and approve/disapprove requests for unclassified and collateral systems.
- Ensure life-cycle security integrity of all SCE ISs.
- Develop procedures necessary to implement higher level regulations and directives.
- Provide guidance and policy to all subordinate SCE organizations.
- Promote the nomination of SCE personnel for NSA/CSS Security Achievement Awards.
- Manage the SCE IS and Network Security Training Program to include:
- Ensure all SCE ISSMs and ISSOs attend the National Cryptologic School OIAC-2225 course, "Operational IS Security" or equivalent.
- Coordinate the training of nominees with the National Cryptologic School.
- Publish SCE annual training schedules for the OIAC-2225 course, which is published in October-November for the following calendar year.
- Report name, organization, and address of all students to the National Cryptologic School for certificates of completion.
- Develop unique SCE courses and materials for training, as necessary.
- Maintain a level of expertise by attending IS and Network security conferences, symposiums, and training courses sponsored by other agencies.
- Augment SCE inspections, both Inspector General (IG) and others, upon request.
- Review requirements for approving public-domain software before its use on any SCE IS.

1.5.7 (U) Commander/Commanding Officer (CO)/Senior Intelligence Officer (SIO) Responsibility

Commanders/CO/SIOs, in conjunction with their ISSM/ISSOs/System Administrators (SA), will work together to present a cohesive training program, both for users and IS & network security personnel. If well developed and effectively implemented, the security program can help mitigate IS security threats, help prevent the compromise or loss of classified information, and produce users who act effectively to secure system resources. The responsibilities of the Commander/CO/SIO, as prescribed in DCID 6/1, paragraph 1.1.16, and DoD 5105.21-M-1, Chapter 1, include:

- Appointment of an ISSM in writing and, where applicable, ensure a copy of orders are forwarded to the SCE organization's ISSPM or the DIA DAA Rep/SCO.
- Ensure the establishment and fund of an effective and responsive IS Security (ISS) Program.

- Participate as an active member of the organization's CCB or appointment of a representative to act in their absence.
- Ensure that users and ISS personnel receive DoD-mandated certification training IAW their responsibilities as part of an approved ISS training program.
- Ensure ISS policies are enforced and implemented.

1.5.8 (U) Information Systems Security Manager (ISSM)

The ISSM is appointed in writing by the authority at a site responsible for information system security. ISSM responsibilities should not be assigned as collateral duties. The ISSM shall:

- Be a U.S. citizen;
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system; and
- Attend DAA approved training.

The ISSM responsibilities include:

- Forward a copy of his/her appointment letter to the DAA Rep/SCO.
- Develop and maintain a formal IS security program.
- Implement and enforce IS security policies.
- Oversee all ISSOs to ensure they follow established IS policies and procedures.
- Ensure ISSM/ISSO review weekly bulletins and advisories that impact security of site information systems to include, AFCERT, ACERT, NAVCIRT, IAVA, and DISA ASSIST bulletins.
- Ensure that periodic testing (monthly for PL-5 systems) is conducted to evaluate the security posture of the ISs by employing various intrusion/attack detection and monitoring tools (shared responsibility with ISSOs).
- Ensure that all ISSOs receive the necessary technical (e.g., operating system, networking, security management, SysAdmin) and security training to carry out their duties.
- Assist ISSOs to ensure proper decisions are made concerning the levels of concern for confidentiality, integrity, and availability of the data, and the protection levels for confidentiality for the system.
- Ensure the development of system accreditation/certification documentation by reviewing and endorsing such documentation and recommending action to the DAA Rep/SCO.
- Ensure the development of documentation if site accepts IS without all appropriate C & A documents.
- Ensure approved procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output.
- Maintain, as required by the DAA Rep/SCO, a repository for all system accreditation/certification documentation and modifications.
- Coordinate IS security inspections, tests, and reviews.
- Investigate and report (to the DAA/DAA Rep and local management) security violations and incidents, as appropriate.

- Ensure proper protection and corrective measures have been taken when an IS incident or vulnerability has been discovered.
- Ensure data ownership and responsibilities are established for each IS, to include accountability, access and special handling requirements.
- Ensure development and implementation of an effective IS security education, training, and awareness program.
- Ensure development and implementation of procedures IAW configuration management (CM) policies and procedures for authorizing the use of hardware/software on an IS. Any additions, changes or modifications to hardware, software, or firmware must be coordinated with the ISSM/ISSO and appropriate approving authority prior to the addition, change or modification.
- Develop procedures for responding to security incidents, and for investigating and reporting (to the DAA Rep/SCO and to local management) security violations and incidents, as appropriate.
- Serve as a member of the configuration management board, where one exists (however, the ISSM may elect to delegate this responsibility to the ISSO.)
- Working knowledge of system functions, security policies, technical security safeguards, and operational security measures.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

1.5.9 (U) Information Systems Security Officer (ISSO)

The ISSO shall:

- Be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

Responsibilities of the ISSO shall include:

- Ensure systems are operated, maintained, and disposed of in accordance with internal security policies and procedures as outlined in the accreditation/certification support documentation package.
- Attend required technical (e.g., operating system, networking, security management, SysAdmin) and security training relative to assigned duties.
- Ensure all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.
- Ensure that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level of the system.
- Report all security-related incidents to the ISSM.
- Initiate protective and corrective measures when a security incident or vulnerability is discovered, with the approval of the ISSM.
- Develop and maintain an accreditation/certification support documentation package for system(s) for which they are responsible.

- Conduct periodic reviews to ensure compliance with the accreditation/certification support documentation package.
- Ensure CM for IS software and hardware, to include IS warning banners, is maintained and documented.
- Serve as member of the Configuration Management Board if so designated by the ISSM.
- Ensure warning banners are placed on all monitors and appear when a user accesses a system.
- Ensure system recovery processes are monitored and that security features and procedures are properly restored.
- Ensure all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notify the ISSM and the DAA Rep/SCO when a system no longer processes classified information.
- Formally notify the ISSM and the DAA Rep/SCO when changes occur that might affect accreditation/certification.
- Ensure system security requirements are addressed during all phases of the system life cycle.
- Follow procedures developed by the ISSM, IAW CM policies and procedures, for authorizing software use prior to its implementation on a system. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM and appropriate approving authority prior to the change.
- Establish audit trails and ensure their review.
- Ensure user identification (USERID) and authentication mechanisms of the IS or network are established.
- Ensure the most feasible security safeguards and features are implemented for the IS or network.
- Ensure no attempt is made to strain or test security mechanisms, or perform network line monitoring, or keystroke monitoring without appropriate authorization.
- Perform network monitoring for the purpose of identifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

1.5.10 (U) The Program Management Office (PMO)/Program Manager (PM)

- The PM/PMO shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

The responsibilities of the PMO/PM will include**:**

- Ensure compliance with current IA policies, concepts, and measures when designing, procuring, adopting, and developing new ISs. This includes systems that are developed under contracts with vendors or computer services organizations and includes those systems that store, process, and/or transmit intelligence information.

- Appointment of an Information System Security Engineer (ISSE)/System Design Security Officer (SDSO) in writing, to ensure system design is developed and implemented with required security features and safeguards; ensure enhancements to existing systems provide equal or improved security features and safeguards; consult with the appropriate certifying organization(s) as early as possible.
- Ensure that the CM process is addressed and used when new SCI ISs are under development, being procured, or delivered for operation. An integral part of CM is the System Accreditation process. Therefore, it is imperative that accreditation authorities be advised of CM decisions. This will ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is being incorporated into system designs. This participation is most important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR).
- Ensure a risk assessment on the IS while under development and keep the risk assessment current throughout the acquisition/development portion of the life cycle.
- Enforce security controls that protect the IS during development.
- Ensure all steps involved in the acquisition and delivery of a certifiable IS followed. These include:
- Evaluate interoperability with other systems.
- Describe the IS mission so that it is clearly understood.
- Formulate a concept and design for meeting the security requirements.
- Incorporate security requirements during system development.
- Develop accreditation support documentation to be fielded with the IS.
- Ensure the IS undergoes Certification and/or Accreditation (C&A) Testing and Evaluation (T&E) prior to operation.
- Coordinate a C&A schedule with the DAA or DAA Rep.

1.5.11 (U) Privileged Users (e.g., System Administrator [SA])

The responsibilities inherent to IS administration are demanding and require a thorough knowledge of the IS. These responsibilities include various administrative and communications processes that, when properly carried out, will result in effective IS utilization, adequate security parameters, and sound implementation of established IA policy and procedures. System administrators shall:

- Be U.S. citizens;
- Be IA trained and certified in compliance with DoD requirements; and
- Hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system.

In addition to the requirements for a general user, responsibilities of system administration personnel shall include:

- Implement the IS Security guidance and policies as provided by the ISSM/ISSO.
- Maintain IS and networks to include all hardware and Commercial Off-The-Shelf/Government Off-The-Shelf software (COTS/GOTS).
- Monitor system performance ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored.

- Report all security-related incidents to the ISSM/ISSO.
- Ensure that all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.
- Perform equipment custodian duties by providing other system unique requirements that may be necessary. Ensure systems are operated, maintained, and disposed of IAW internal security policies and procedures outlined in the accreditation/certification support documentation package.
- Maintain software licenses and documentation.
- Notify the ISSM/ISSO formally when changes occur that might affect accreditation/certification.
- Ensure CM for security-relevant IS software and hardware, to include IS warning banners, is maintained and documented.
- Monitor hardware and software maintenance contracts.
- Implement USERID and authentication mechanisms of the IS or network and issue user logon identifications and passwords.
- Ensure adequate network connectivity by ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.
- Maintain audit trails and conduct reviews and archives as directed by the ISSM/ISSO.
- Provide backup of system operations.
- Assist the ISSM/ISSO in developing and maintaining accreditation/certification support documentation package for system(s) for which they are responsible.
- Participate in periodic reviews to ensure compliance with the accreditation/certification support documentation package.
- Ensure all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notify the ISSM/ISSO when a system no longer processes classified information.
- Follow procedures developed by the ISSM/ISSO, authorize software use before implementation on the system.
- Assist the ISSM/ISSO in maintaining configuration control of the systems and applications software ensuring the most feasible security safeguards and features are implemented on the IS or network.
- Prohibit attempts to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring without appropriate authorization.
- Perform network monitoring for the purpose of correcting deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority and advising the ISSM/ISSO of security anomalies or integrity loopholes.
- Participate in the Information Systems Security incident reporting program and with the approval of the ISSM/ISSO, initiate protective or corrective measures when a security incident or vulnerability is discovered.

1.5.12 (U) General Users

General users must hold U.S. Government security clearance/access approvals commensurate with the highest level of information processed by the system. The responsibilities of a general user shall include:

- Use the system for official use, only. Appropriate personal use of IS must be approved first by the individual's supervisor.
- Participate, at a minimum, in annual computer security awareness briefings/training.
- Provide appropriate caveat and safeguard statements on all IS files, output products, and storage media.
- Protect ISs and IS peripherals located in his/her respective areas.
- Secure unattended ISs by invoking screen lock or logging off.
- Safeguard and report any unexpected or unrecognizable output products to the ISSO/SA as appropriate. This includes both display and printed products.
- Safeguard and report the receipt of any media received through any channel to the appropriate ISSO/SA for subsequent virus inspection and inclusion into the media control procedures.
- Report all security incidents to the ISSO/SA or ISSM.
- Protect passwords at the same level as the highest classification of material which the system is accredited to process.
- Protect passwords by never writing passwords down and destroy the original password documentation following initial review.
- Protect passwords from inadvertent disclosure.
- Protect all files containing classified data.
- Notify the system ISSO/SA if he or she suspects that a possible IS and/or network security problem exists.
- Ensure access doors, covers, plates and TEMPEST seals are properly installed on ISs to eliminate security hazards.
- Protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

1.5.13 (U) Prohibited Activities

In general, there are activities that all users shall not perform on Government systems:

- Use ISs for personal gain, personal profit or illegal activities.
- Release, disclose, or alter information without the consent of the data owner or the disclosure officer's approval. Violations may result in prosecution of military members under the Uniform Code of Military Justice, Article 92 or appropriate disciplinary action for civilian employees.
- Attempt to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring without proper authorization.
- Attempt to bypass or circumvent computer security features or mechanisms.

- Modify the system equipment or software or use it in any manner other than its intended purpose.
- Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.
- Introduce malicious code into any IS or network and will comply with rules and regulations for scanning all magnetic media that he/she introduces, mails, or transports into or out of the organization.

1.6 (U) CONFIGURATION CONTROL BOARD (CCB) OVERSIGHT

This document is under the purview of a Joint Service CCB consisting of representatives from DIA, NIMA, NSA/CSS and its SCEs, and the SCOs. Any recommended changes to this document should be forwarded to the appropriate CCB member.

1.7 (U) OTHER DOCUMENTATION SUPERSESSION

This document supersedes all previous editions of the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards.

CHAPTER 2 - LIFE CYCLE SECURITY

2.1 (U) PURPOSE

The Director of Central Intelligence Directive (DCID) 6/3, for the Intelligence Community is used to provide a system of evaluating the degree of trust needed for an IS processing classified and sensitive information. It is the basis for specifying security requirements in acquisition specifications, both for existing and planned systems. The Program Manager (PM), during acquisition/development, will require that security be an integral part of any contract used for acquisition consistent with the security requirements of the system. The PM and IS developers involved in the acquisition process of new ISs must ensure these new systems function as intended and are accreditable. They must ensure that systems are designed to meet user requirements, are developed economically, and contain appropriate security controls and audit trails. C&A procedures must be precisely followed to ensure new ISs are created and can be readily approved for operation at an acceptable level of risk. Acquisition procedures must address all aspects of IS development, to include the security requirements that must be met, the IS security features required, the IS operating environment, and a plan that properly tracks the process by which IS definition, development, and security testing are to take place. The purpose of this chapter is to address acquisition security requirements and includes:

- National security policy requirements as they pertain to system development.
- The responsibilities involved in the accreditation process.
- Levels of Concern and Protection Levels.
- Guidance that appropriate security requirements are identified early in the acquisition process.

2.2 (U) SCOPE

The early and complete identification of security requirements for an Information System is a major security objective in all phases of the IS life cycle. These guidelines apply to all security personnel who must consider, improve, or change security throughout the life cycle to ensure continued adequate protection. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

2.3 (U) PROCEDURES

Within each organization, life-cycle security requirements will be related to one of the seven life cycle phases which apply to all systems: Government owned, leased, or on loan from other organizations. DAA Reps/SCOs must review and approve detailed system or subsystem security specifications.

2.3.1 (U) Concepts Development Phase

During the conceptual phase, the Developer, User and DAA determine the criticality of the IS being planned based on the data sensitivity determined by the data owner. This is accomplished by conducting sensitivity, risk/threat, interoperability**,** and economic assessments. The results of these

assessments provide the data necessary to perform the analysis and design of the next phase. These guidelines apply to all personnel performing acquisition of ISs with the objective of fielding ISs with the appropriate security requirements identified early in the acquisition process.

2.3.1.1 (U) IS Security Design

The PMO/PM ensures all IS security requirements are incorporated in the Critical Design Review, the SSP/Systems Security Authorization Agreement (SSAA) and the Security Concept of Operations (SECONOPS) (see DCID 6/3, 4.B.1.c.(1)). The PMO/PM and their SDSO/ISSE, will ensure the IS security design meets the requirements of DCID 6/3.

2.3.1.2 (U) Statement of Work (SOW) Requirements

The SOW will include a DD Form 254 and address contractor related issues pertaining to contractor personnel security, physical security, contractor ISs in support of the contract, TEMPEST requirements, and applicable security regulations. A Government official, either the SDSO/ISSE or DAA Rep/SCO, will coordinate these specific requirements depending on the particular acquisition.

2.3.1.3 (U) Additional Documentation

Additional documentation based on the system's identified Protection Level to include guide(s) or manual(s) for the system's privileged users (test plans, procedures and results) and a general user's guide may be required.

2.3.2 (U) Design Phase

The DAA/DAA Rep along with the data owner guidance determines the Levels of Concern (LOC) for Confidentiality, Integrity and Availability based on the information characteristics determined in the Concepts Development Phase. The DAA/DAA Rep then determines the required Protection Level based on the need-to-know, formal access approval(s), and clearance level(s), if applicable, of system users as compared to the sensitivity, formal compartments, and classification of the data to be stored, processed, or transmitted on the system. The Levels of Concern and Protection Levels are:

Security Features	**Level of Concern**	**Protection Levels**
Confidentiality	High (Basic/Medium not used in Intelligence ISs)	PL-1, PL-2, PL-3, PL-4, PL-5
Integrity	Basic, Medium, High	
Availability	Basic, Medium, High	

2.3.2.1 (U) Levels-of-Concern

Based on the characteristics of the information in the IS, a Level-of-Concern must be determined in each of three categories: confidentiality, integrity, and availability. The available Level-of-Concern ratings are Basic, Medium or High. The DAA determines the Level-of-Concern separately for each category based on the following:

- The Confidentiality Level-of-Concern rating for all ISs that process intelligence information is, by definition, High.
- The Integrity Level-of-Concern is determined by the necessary degree of resistance to unauthorized modification of the data in the IS. The greater the need for data integrity, the higher the Level of Concern.

- The Availability Level-of-Concern rating is based on the need of ready access to the system data. The greater the need for rapid data availability, the higher the Level-of-Concern.
- A detailed description of the determination and assignment of Levels-of-Concern can be found in DCID 6/3, section 3.B. and Table 3.1, with even greater detail of each category in Chapters 4 (Confidentiality), 5 (Integrity), and 6 (Availability).

2.3.2.2 (U) Protection Levels

The Protection Level of an IS is the implicit level of trust placed on the procedures and technical capabilities of the system, and applies only to confidentiality. After determining that the Level-of-Concern for confidentiality must be high (since the system processes intelligence data), the DAA must then determine the necessary Protection Level based on:

- Required clearances,
- Formal access approval, and
- Need-to-know of all IS users.

2.3.2.2.1 (U) IS Protection Level Determinations

The DAA/DAA Rep and data owner must explicitly determine the Protection Level for each IS to be accredited. DCID 6/3, Section 3.C. and Table 4.1 differentiate between the five Protection Levels (PL1 – PL5). Chapter 4 details the security features required for each Protection Level.

2.3.2.2.2 (U) Security Documentation (SSP/SSAA) Requirements

The LOCs for Integrity and Availability and the PL for Confidentiality are identified using DCID 6/3 Chapters 4-6. During the design phase, the Project Management Office (PMO) ensures development of the Security Requirements Traceability Matrix (SRTM) and the continued development of the SSP/SSAA. This is a living document and should be updated throughout the IS's life cycle. It incorporates security documentation requirements found in DCID 6/3 and includes the mission need, system and environment description, intended system users, system security requirements, and development schedule. A template for the SSAA can be found in the DoD Intelligence Information System (DoDIIS) Security Certification and Accreditation Guide, Appendix D. A template for the SSP can be found in the NSA/CSS Information System Certification and Accreditation Process (NISCAP). The initial draft of the SSAA/SSP must be approved by the DAA Rep/SCO prior to system development. Actions must be taken by the Program Managers (PM) and SDSO/ISSE to ensure compliance with directives according to DCID 6/3.

2.3.3 (U) Development Phase

Adequate implementation of the necessary security measures is ensured during the development phase. The SDSO/ISSE, appointed by the PMO, has the major responsibility during the development phase. SDSO/ISSE ensures a test plan is prepared IAW the SRTM and participates in all project meetings including site surveys as appropriate. Security support from the certifying organization is required based on the Protection Level of the IS. Hardware, software, telecommunications and the entire operational environment must comply with the SSP/SSAA. This extends beyond the system itself; the proposed or existing facility that will house the system must be considered to ensure that proper physical security is available. During the development phase, design reviews may identify security considerations that were overlooked in the initial system

design. If so, the SSAA/SSP must be updated accordingly. If major security considerations are discovered, the development may return to a previous phase for rework.

2.3.4 (U) Test, Certification and Accreditation Phase

During the test phase, the entire system is critically reviewed to ensure compliance with all specified measures. Security testing is conducted to certify that the system's security and contingency operations are properly implemented. Any shortcomings and/or vulnerabilities are identified, and a risk analysis is conducted. Based upon the outcome of the risk analysis, a plan addressing the shortcomings (fixes, work-arounds, etc.) is developed. All this is detailed in a Report, which is used by the DAA/DAA Rep when making the approval decision. A template for the test report is located in the DoDIIS Security Configuration and Accreditation Guide, and the NISCAP. Following the conclusion of security testing, the resolution of any shortcomings, and after the appropriate DAA/DAA Rep grants certification approval, the system is released for operational use.

2.3.4.1 (U) Time Line for Certification Activities

The timeline for certification activities will be coordinated with the certifying organization. A minimum 90-day period is the basis for providing enough time for certifiers to properly prepare for and conduct a system certification evaluation and recommendation to the DAA/DAA Rep. The 90 day timetable begins with the submission of the Request for Certification from the Program Manager (PM/PMO) to the certifying organization.

	90 days	**60 days**	**30 days**	**0 days**
PM Request for Certification/Accreditation	**X**			
SSAA/SSP	**X**			
SCE/SCO approval of SSAA/SSP		**X**		
SRTM & Test Procedures (SFUG if necessary)		**X**		
SCE/SCO approval of Test Procedures			**X**	
SCE/SCO submits Test Report and Test Memo				**X**

2.3.5 (U) Deployment and Operations Phase

Once the system is operational, the site operations staff and ISSO/ISSM are responsible for monitoring its security. They do this by controlling changes to the system via strict Configuration Management. IS users are responsible for operating the system in compliance with the security guidelines found in the SSAA/SSP. As required by DCID 6/3, the DAA/DAA Rep periodically reviews the adequacy of system security as required by all applicable regulations for unclassified, sensitive-unclassified, collateral, and SCI material. This review will take into account any system modifications and changes, including both hardware and software, to ensure that security requirements are adequate to meet any identified risks, threats to, or vulnerabilities of the system. All changes are updated in the SSAA/SSP as they occur. If any changes significantly affect the system's security posture, the DAA/DAA Rep is notified so that the need for recertification/reaccreditation can be determined.

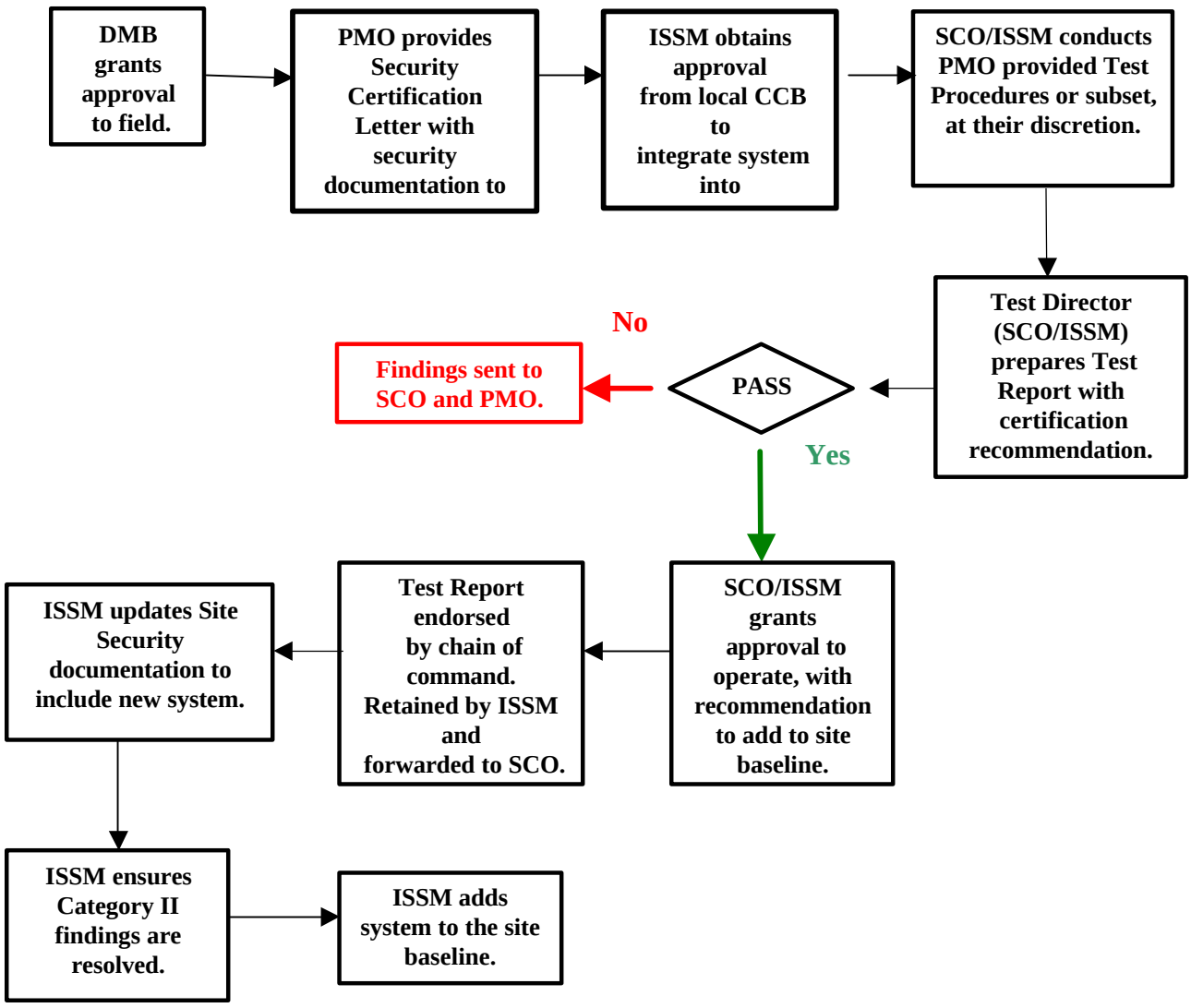


Figure: 2.1 – Example process for PL2 DoDIIS IMA after approval to field.

2.3.6 (U) Contingency Planning

Once a system is deployed to a site a contingency plan for emergency response, backup operations, and post-disaster recovery is to be maintained by the activity as a part of its security program. It consists of a comprehensive statement of all the actions to be taken before, during, and after a disaster or emergency condition along with documented and tested procedures. It ensures that critical resources are available and facilitates the continuity of operations in an emergency situation.

- **Backup.** Preventing catastrophic loss of data and progress requires that users maintain adequate backups for their stored data. Besides preventing data loss, backups of data for archiving purposes allow for proper on-line storage management. All magnetic media must be properly labeled and protected according to Chapter 13.
- **Responsibilities.** Each ISSM, or designee, will develop locally needed backup plans. The plans should consider data-production rates and data-loss risks when under development. The areas of risk that should be identified and planned for are:

- **Immediate Losses.** Ensures that the risk of a power failure and the resulting loss of data is worked at the time of power loss. Develop policy and procedures that reflect these risks. For example, if one were creating a word-processing document when power loss occurred, the document would be lost if the user had not made periodic "saves" while creating it. Some word-processing systems allow the user to make periodic saves automatically (for example, Word for Windows). Most applications do not have this capability, and the users must be made aware of this potential problem.
- **Media Losses.** Develop a local procedure that reflects this risk. If a hard disk were dropped or contaminated in some way, the disk backups, coupled with periodic incremental backups between full backups, would allow you to restore the data close to the condition it was in before the loss. Keep "active backups" for disks that contain often-used applications.
- **Archiving Inactive Data.** Develop procedures to manage the disk space. For example, old correspondence might be put onto a disk for archiving purposes. Thus, you could create a list of all files and file descriptions which could be returned to the active users.

2.3.7 (U) Recertification/Reaccreditation Phase

As required by the DAA/DAA Rep, a system must be recertified/reaccredited whenever security changes occur in the LOC and PL, technical or non-technical security safeguards, threats to the system, operational environment, operational concept, interconnections, or any other significant increases in the level of residual risk. This process includes: a review of existing security documentation to verify that these documents still accurately represent the system, a reevaluation of the system vulnerabilities, threat and risk, and a complete security test, or subset of the original security test will be conducted. Even if no security-significant changes occur, recertification/reaccreditation of a system must be re-evaluated every three years after the issuance of an accreditation. Site Based accreditation provides for continued reevaluation.

2.3.8 (U) Disposal Phase

When an IS is no longer needed disposition can occur in several ways.

- purging information residue from an IS or a component
- releasing the IS or a component for reuse within the Intelligence Community
- destroying an IS or a component through authorized channels, or
- the method of shipment for an IS or component.

DAA/DAA Rep and the appropriate data owners must approve all of the above actions. While emergency destruction of an IS is a possibility that occurs during the normal operational phase, it is considered a special case during the disposal phase.

CHAPTER 3 - SIGNALS INTELLIGENCE (SIGINT) SYSTEMS ACCREDITATION PROCESS AND PROCEDURES

3.1 (U) PURPOSE

This chapter provides certification and accreditation processing guidelines and procedures for cryptologic information systems that process information under the purview of the Director, National Security Agency (DIRNSA). It does not apply to intelligence information systems that fall under the cognizance of other PAA's such as the Director, Defense Intelligence Agency (DIA).

3.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

3.3 (U) DISCUSSION

3.3.1 (U) Accreditation

Accreditation is the official management decision to permit operation of an Information System (IS) in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

3.3.2 (U//FOUO) NISCAP

The NSA/CSS Information Systems Certification and Accreditation Process (NISCAP) is the NSA/CSS structured engineering process for achieving security certification and accreditation for systems designed to process information under the purview of the DIRNSA. In accordance with NSA/CSS Manual 130-1, all SIGINT systems must be formally accredited under the NISCAP before they can be declared operational and allowed to process, store, transmit, or receive data of any classification. The NISCAP facilitates compliance with the separate Certification and Accreditation (C&A) policies of the Intelligence Community (IC) and the DoD. This process as collaborated in the DK1 NISCAP Guide will be followed by Program Managers (PM), System Developers and all other C&A participants to ensure that systems under development or undergoing modifications are certifiable and accreditable for use in environments where DIRNSA is the PAA.

3.3.3 (U) Configuration Management

The accreditation process and associated security concerns are integral to configuration management enforcement. Therefore, ISSPM, ISSMs or ISSOs will be included in configuration management decisions to ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is incorporated into system designs. This participation is very important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR). Where

there is no formal configuration management process in an acquisition or system modification, the PM will coordinate all relevant activities with the accreditation authority.

3.4 (U) NISCAP FLOW

Figure 3.1, graphically depicts the NISCAP. As the figure indicates, the process may be initiated from one of three different logical points: Unit, SCE, and the NSA/CSS.

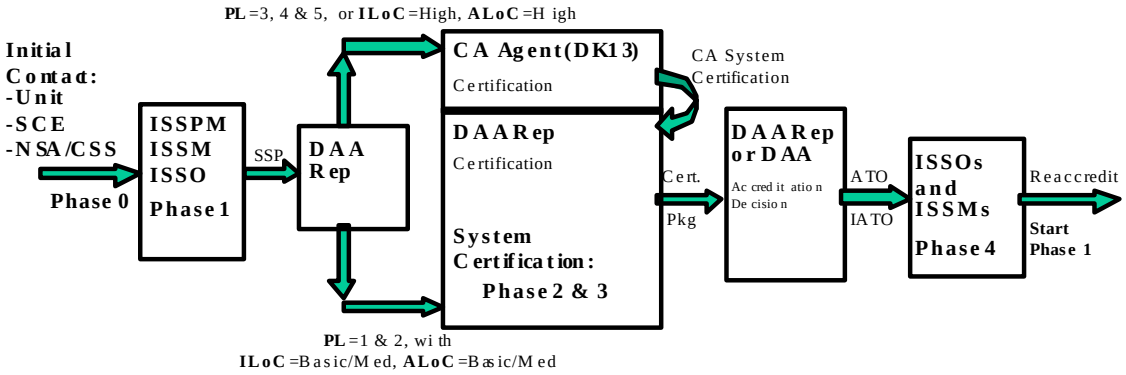


Figure 3.1 (U) National Security Agency/Central Security Service Information System Certification And Accreditation Process

3.4.1 (U) General Accreditation Approvals

The NSA/CSS DAA has delegated to the DAA Representatives the authority to accredit systems that operate at Protection Level 1 (PL 1) or Protection Level 2 (PL 2). This includes granting either an Approval to Operate (ATO) or an Interim Approval to Operate (IATO). Before a cryptologic IS can be granted an ATO, a site visit by the DAA/DAA Representative is required. Activities during the site visit include testing and evaluation of the system's security safeguards/controls in it's operational environment and assessment of the organization's security procedures. The DAA representative may use the Site Accreditation Visit Checklist, Appendix F (NSA/CSS NISCAP Guide) as a guide. If, following the site visit, the DAA/DAA Representative determines that sufficient security safeguards exist, the system is in compliance with DCID 6/3 security requirements, and it operates at an acceptable level of risk, a three-year ATO is normally granted.

3.4.2 (U) Interim Approval to Operate (IATO)

The DAA Representative may issue an IATO for a PL 1 or PL 2 system, to allow it to operate until a site visit can be scheduled, provided sufficient safeguards are documented in the System Security Plan (SSP). The DAA/DAA Representative may also issue an IATO for a PL 1 or PL 2 system if, during the site visit, minor security deficiencies are identified and the organization requires time to implement corrective measures. A follow-up site visit to verify that the deficiencies have been corrected may or may not be required; this is at the discretion of the DAA/DAA Representative. Interim approvals to operate may be issued for a period of up to 180 days. If required, the DAA/DAA Representative may extend the IATO one time for an additional 180 days. The initial IATO and extension cannot exceed a total of 360 days.

3.4.3 (U) Reaccreditation

When security-relevant changes, as determined by the ISSPM, are made to an accredited IS, the SSP and other NISCAP documentation must be updated by the ISSO/ISSM to reflect the change(s) and resubmitted by the ISSM to the appropriate DAA Representative. Failure of an ISSO or ISSM to identify system changes in the SSP and other NISCAP documentation may result in the system's accreditation being rescinded. The following are examples of changes that are grounds for re-accreditation:

- The Central Processing Unit (CPU) and/or operating system changes.
- The IS is relocated to another area or TEMPEST zone.
- The IS Protection Level (PL) changes.
- The Accredited Security Parameter (ASP) changes.
- The IS is connected to another IS or network.
- Users, whose clearances are not commensurate with the classification of the IS, are added to the network.

3.4.4 (U) Rescinding Accreditations

The DAA/DAA Representative may rescind the accreditation of an Information System (IS), if violations are identified. There are, however, some system changes that do not constitute the need for rescinding an accreditation. They are as follows:

- The substitutions of similar components while components are in maintenance. However, if the original CPU is not returned to the Information System (IS) when repair is completed, then an update to the SSP must be accomplished to reflect the correct make, model, and serial number of the replacement CPU.
- The addition of new terminals (of same configuration), peripheral devices, or relocation of an Information System (IS) providing the SSP is updated within 90 days to reflect the system additions or relocation. These actions can only be done with appropriate coordination (TEMPEST, Physical Security Office, etc.) and with ISSM approval.

3.4.5 (U) Accreditation Three-Year Anniversary Review

Each IS accreditation will be reviewed every three years. The ISSM is responsible for ensuring that the recertification and reaccreditation of each accredited IS is completed upon its 3-year anniversary. The SSP and other NISCAP documentation will be updated to reflect any undocumented changes and will be coordinated with ISSPM and forwarded to the appropriate DAA/DAA Representative for accreditation.

3.4.6 (U) Information Systems (IS) Exempted from Accreditation under NISCAP

Computers that have never been exposed to, contained, or processed cryptologic information are exempt from accreditation under NISCAP. The following listed types of equipment/systems may be exempt provided they have never been exposed to, contained or processed Cryptologic information:

- Computerized test equipment.
- Computers used in driving drill presses and their operations.

- Computers used in engraving devices or machines.

3.4.7 (U) TEMPEST

Refer to Chapter 5 for applicable TEMPEST procedures involved with IS accreditation. It is imperative that all cryptologic ISs operate with appropriate approval and with the security controls necessary to protect the information they process. The ISSOs, ISSMs, ISSPMs and DAA Representatives will ensure that certification and accreditation processes and procedures as defined in NISCAP are followed.

3.5 (U) Requests for Accreditation

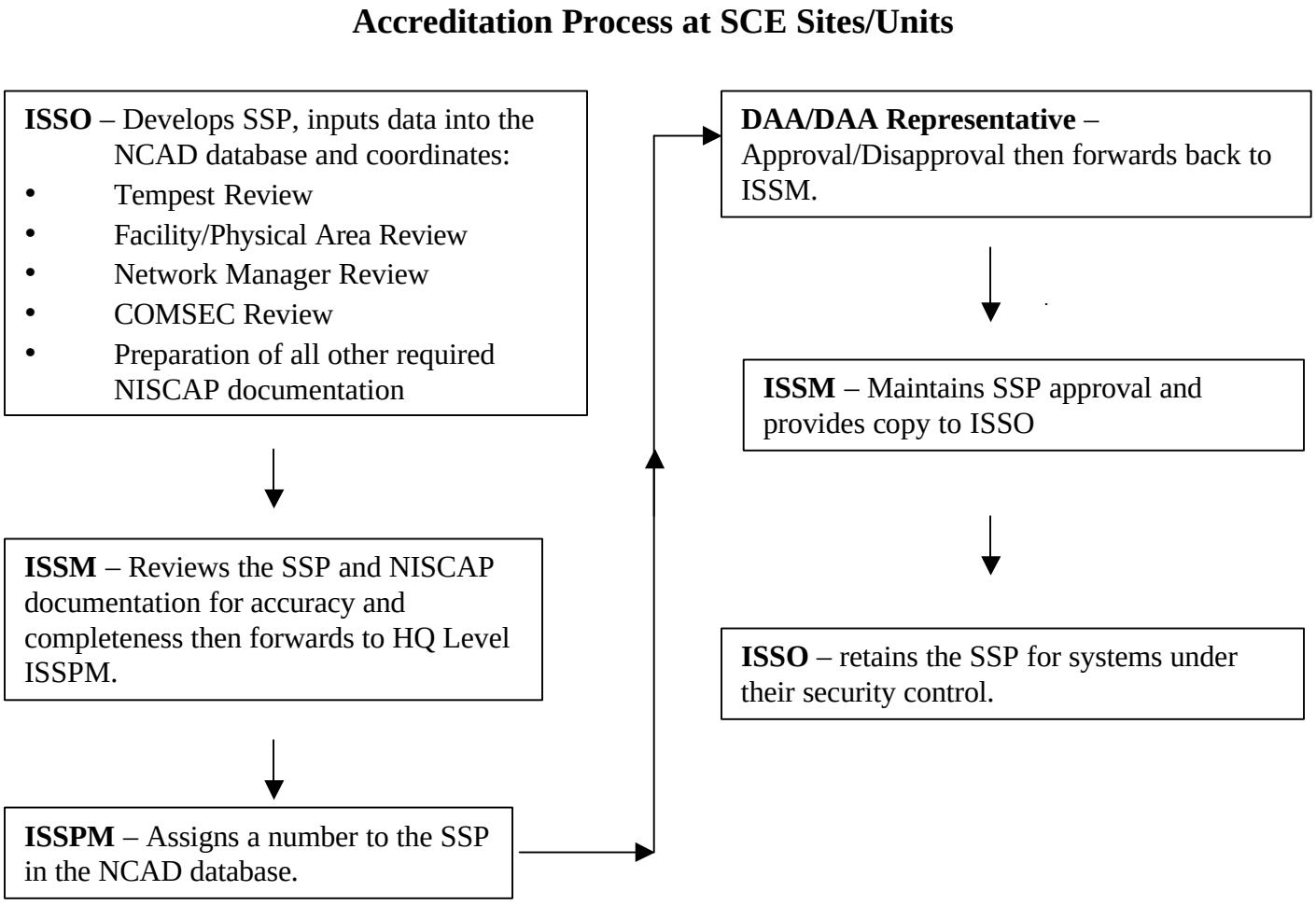


Figure 3.2 Accreditation Process at SCE Sites/Units

3.5.1 (U) Accreditation Requests Initiated at the Unit Level for PL 1 and PL 2 ISs with only Basic/Medium Integrity Level of Concern (ILoC)/Availability Level of Concern (ALoC)

When an ISSO/SA becomes aware that a new PL 1 or PL 2 Information System has only Basic/Medium ILoC/ALoC and is going to be obtained through NSA approved acquisition channels, the following should occur. A NISCAP Phase 1 meeting will be held and a Phase 1 Meeting Checklist (Appendix E of the NISCAP Guide) completed. As the details of the IS become available, the required NISCAP documentation, which includes an SSP for the new system, is to be

developed by the ISSO, coordinated through appropriate channels (TEMPEST Officer, SCIF Manager, Physical Security Office), entered into the NSA/CSS Certification Accreditation Database (NCAD), and forwarded to the ISSM for review. The ISSM ensures that the SSP has been properly coordinated, and that the SSP and other NISCAP documentation are accurate and complete. Once entered into the NCAD Database, the SSP and documentation is electronically forwarded by the ISSM to the appropriate ISSPM who does a final review of the SSP, provides the SSP a number and forwards it along with the other NISCAP documentation to the DAA Representative.

3.5.1.1 (U) ISSM review of PL 1 and PL 2 Documentation

It is essential that the ISSM review the PL 1 and PL 2 SSPs and all other NISCAP documentation before forwarding to the HQ ISSPM to ensure that the SSP is complete and accurate. If, during the review process, the DAA Representative finds relevant data missing or not clearly defined, he/she may non-concur and send the SSP and/or other NISCAP documentation back to the ISSM for correction. This can create delays that impact operational requirements.

3.5.2 (U) Accreditation Requests Initiated at the Unit Level for PL 3, PL 4, PL 5

When an ISSO/System Administrator (SA) becomes aware that a new PL 3, PL 4, PL 5 or High ILoC/ALoC IS is being planned for fielding under their purview, the following should occur. The ISSO/SA must inform their ISSM who in turn will inform their ISSPM. The ISSPM will inform their DAA Representative as well as the NSA/CSS Senior Information Systems Security Program Manager (SISSPM), Chief DK14. The SISSPM is directly responsible for administrative and operational actions regarding key component, SCEs and regional ISSPMs. The SISSPM will provide NISCAP guidance, ensure that the process is properly initiated and ensure that the Program Management/Project Office is pursuing certification and accreditation of the system in accordance with NISCAP.

3.5.3 (U) Downward-Directed Accreditation from Program Management/Project Offices

For cryptologic ISs being fielded under the cognizance of a program management or project office, the fielding office must ensure the fielded system is certifiable and meets regulatory requirements. It is also the fielding program management or project office's responsibility to provide the recipient organization with an SSP and all other required C&A documentation pertinent to the system and its operation. The organization's ISSO/ISSM is responsible to add any site or personnel specific information to complete the SSP and or other documentation and then forward it to the appropriate DAA Representative. The fielding organization must coordinate Information System specific issues with the site ISSO/ISSM well in advance of the installation (90 days) if immediate operation is critical. To assist and expedite system installation and operation, the Program Management/ISSO/ISSM will ensure the following guidelines are met:

- The program management/project office fielding the system notifies the recipient organization 90 days prior to scheduled installation and provides accreditation documentation.
- The program management/project office provides prior to, or at time of installation, an accreditation letter issued by the DAA Representative.

Note: The Commander/Commanding Officer/SIO and/or organization ISSO/ISSM may deny access, or refuse country clearance, if overseas, to any team installing an IS without proper certification and accreditation documentation and prior coordination.

3.5.4 (U) Accreditation Requests Initiated at a Single-Service Site

When processing SSPs for PL 1 and PL 2 cryptologic Information Systems (IS), with a Basic/Medium ILoC/ALoC, located in an organization controlled by one military authority for SCIF management, TEMPEST, IS and network security, the SSPs will be handled and coordinated through that authority's chain of command. Accreditation of PL 1 and PL 2 cryptologic ISs, with only a Basic/Medium ILoC/ALoC, that belong to a particular SCE can be granted by a NSA approved DAA Representative. When processing PL 3, PL 4, PL 5, and High ILoC/ALoC cryptologic ISs, the NSA/CSS SISSPM is to be contacted to ensure that the certification and accreditation of the system is accomplished in compliance with NISCAP.

3.5.5 (U) Submission of the SSP and NISCAP documentation

A PL 1 or PL 2 cryptologic IS, with a Basic/Medium ILoC/ALoC, cannot be operated without the approval of the appropriate DAA Representative. PL 3, PL 4, PL 5 and High ILoC/ALoC ISs require approval by the NSA/CSS DAA/PAA prior to them being operated. An SSP must be developed, coordinated, entered into NCAD, and all other required NISCAP documentation submitted to the DAA Representative. The SSP and other NISCAP documentation should be submitted not later than 60-90 days prior to the desired Initial Operational Capability (IOC). If the system is in the development stage (NISCAP Phase 2), the SSP and other NISCAP documentation should be submitted during the development process.

3.5.6 (U) Format and Content

The SSP format, as presented by NCAD, will be used for the submission of all cryptologic information system SSPs. The format and content of the other NISCAP documentation will be in accordance with the templates contained in the NISCAP Guide. The minimum Classification of SSPs and documents for cryptologic Information Systems is CONFIDENTIAL.

CHAPTER 4 - DODIIS SITE-BASED ACCREDITATION AND SYSTEM CERTIFICATION

4.1 (U) PURPOSE

The DoDIIS Information Assurance Program has two components: The DoDIIS Systems Security Certification and Accreditation Process and the DoDIIS Site-Based Accreditation Methodology. This applies to all systems that process, store, or communicate intelligence information under the purview of the Director, DIA. Note: This chapter does not apply to intelligence information systems under the cognizance of the Director, NSA/CSS. The DoDIIS Systems Security Certification and Accreditation (C&A) Process addresses information systems being developed or undergoing modification that is evaluated prior to being fielded to DoDIIS sites. The DoDIIS Security Certification and Accreditation Guide describes the process for determining the appropriate security requirements that the new or modified system must meet, provides information on the requisite security documentation needed to support system security certification, and outlines the process for testing and fielding systems within the DoDIIS community. All Information Systems within DoDIIS will be tested and evaluated prior to achieving approval to operate or being granted formal certification and fielding to a DoDIIS site. The DoDIIS Site-Based Accreditation Methodology examines and establishes a baseline of all eligible information systems within a defined area, and designates this as a "Site". The Command authority for the site appoints an ISSM, and that individual, in coordination with the cognizant Certification Organization, manages all security related issues impacting the site's accredited baseline. Details of the Site-Based Accreditation Process can be found in DIAM 50-4.

4.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

4.3 (U) SYSTEM CERTIFICATION AND ACCREDITATION PROCEDURES:

4.3.1 (U) System Certification and Accreditation Compliance

The DoDIIS Security Certification and Accreditation Guide requires that all ISs be certified and accredited to ensure the IS meets the documented security requirements and that the security of the IS, as accredited, is maintained throughout its life cycle. The certification process validates that appropriate Levels-of-Concern for Integrity and Availability and an appropriate Protection Level have been selected for the IS from the descriptions in DCID 6/3 and the required safeguards have been implemented on the IS as described in the associated security documentation. The DoDIIS security certification and accreditation process has been harmonized with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

4.3.2 (U) System Certification and Accreditation Process

4.3.2.1 (U) Phase 1

Definition – Focuses on understanding the IS requirement, the environment in which the IS will operate, the users of the IS, the security requirements that apply to the IS, and the level of effort necessary to achieve accreditation. The objective of Phase 1 is to agree on the intended system mission, security requirements, C&A boundary, schedule, level of effort, and resources required for the certification effort. This information is captured in the SSAA/SSP, which is developed by the PM.

4.3.2.2 (U) Phase 2

Development and Verification – Focuses on the system development activity and ensures that the system complies with the security requirements and constraints previously agreed during definition phase.

4.3.2.3 (U) Phase 3

Validation and Testing – Confirms compliance of the IS with the security requirements stated in the SSAA/SSP. The objective of this phase is to produce the required evidence to support the DAA in making an informed decision whether or not to grant approval to operate the system with an acceptable level of residual security risk. This includes system testing (Alpha, Beta-I and Beta-II).

4.3.2.4 (U) Phase 4

Post Accreditation – This phase starts after the system has been certified and accredited for operation. The Post Accreditation phase includes several activities to ensure an acceptable level of residual security risk is preserved. These activities include security documentation, configuration management, compliance validation reviews, and monitoring any changes to the system environment and operations. Changes to the security configuration of the system will require security review by the DAA.

4.3.3 (U) DoDIIS Certification and Accreditation for Exercise or Experiment Scenarios

The DoDIIS certification process for exercise/experiment will vary somewhat from the standard requirements. Lessening of the requirements for exercises/experiments is based on time/risk limitations, on the limited duration, and consequences from security incidents should be negligible, since most information being processed will be exercise traffic. Any approval or IATO is for the duration of the exercise/experiment only. An IATO is not to be construed as an automatic approval for future operational use, unless otherwise specified by approving authority. The criteria for determining which requirements apply are based on 1. Simulated Network (i.e., no live connections); 2. JWICS live only; and 3. Live JWICS and other networks. The following gives a break out of the requirements for differing criteria

4.3.3.1 (U) Simulated Network Connectivity

If the exercise/experiment architecture is using simulation network connectivity (i.e., simulated JWICS (SCI), SIPRNET (Secret), etc.), then the requirements will be as follows:

- SSAA (Abbreviated per SCO/Local ISSM)
- System Architecture/Diagrams
- Local ISSM review (Local ISSMs can review/approve PL2 exercise systems with SCO concurrence)

- SCO concurrence

4.3.3.2 (U) JWICS Connection

If JWICS only connection, above applies in addition to below:

- DIA Concurrence

4.3.3.3 (U) Exercise Use of Multiple Operational Network Connectivity

If the exercise/experiment will be using more than one operational/live network connections with limited duration, the following requirements apply:

- SSAA (SRTM, Test Procedures, TFM, etc. is abbreviated per SCO/DIA)
- System Architecture/Diagrams
- MOAs if interconnections
- SCO recommendation
- DAA concurrence/approval

4.4 (U) SITE-BASED ACCREDITATION METHODOLOGY

4.4.1 (U) Site-Based Accreditation Methodology Compliance

The DoDIIS Site-Based Accreditation Process uses management techniques to assess risk by establishing a security domain called a "DoDIIS Site". This concept incorporates Site Security Management as a function of the DoDIIS Site's CM process. A DoDIIS Site Security Baseline defining the systems infrastructure is required and any changes to the baseline must be documented in a timely manner. Before a DoDIIS site can establish a Site Security Baseline and be accredited, all system(s) must go through the security C&A process. The Site Security Baseline begins with the evaluation and accreditation of all individual ISs at the site. All ISs are then consolidated into this single management entity and evaluated as part of the security environment in which they operate. Site-Based Accreditation examines the ability of the organization to maintain a secure site baseline and environment. The maturity of site security policies, procedures, configuration management, system integration management, and risk management determines the site's ability to successfully establish and control a secure baseline. The certification process has a number of steps which, once successfully completed, will result in a Site Accreditation by the Director, DIA (DIRDIA), the PAA for all DoDIIS sites. DIAM 50-4 describes the step-by-step process to perform the Site-Based Accreditation and identifies documentation required to be maintained at the site. Under Site-Based accreditation, the responsible DAA Rep/SCO will have already certified intelligence mission applications entering the site. All other agency systems are considered "Guest" systems at the site (See below for additional guidance on Guest systems).

4.4.2 (U) The Site-Based Accreditation Process

The Site-Based Accreditation process consists of the following:

4.4.2.1 (U) Initial Site Visit (Initial Site Certification Visit)

A Certification Team will initiate the accreditation process by visiting the site. The purpose of this visit is to gather important baseline information. This function may be incorporated or combined in the Site Accreditation and Site Security and Engineering Certification Testing and Evaluation.

4.4.2.2 (U) Site Evaluation Visit

This visit is essentially a Site Security and Engineering Certification Testing and Evaluation and Site Accreditation, and will normally be conducted within 60-90 days following the Initial Site Certification Visit. However, if the site has its site documentation, baseline, and security posture in order, it may be performed during the initial visit. It will consist of system security certification testing and/or security documentation review on each system.

4.4.2.3 (U) Site Compliance Visit (Vulnerability Assessment and Compliance Verification)

This visit includes a vulnerability assessment of the networks, ISs, and linked operational elements. Assessments may be performed remotely or onsite. During official site visits the DAA Rep/SCO ensures that the site properly maintains control of the site security baseline. Vulnerability Assessment and Compliance Verification are normally conducted simultaneously as required.

4.5 (U) CONTRACTOR ACCREDITATION

Contractor facilities will not be site-based. Contractors will submit accreditation documentation IAW the National Industrial Security Program (NISP) Operating Manual (NISPOM) and the DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems, Industry Annex, 12 Apr 02.

4.6 (U) ACCREDITATION REVIEW

The ISSM is responsible for ensuring that the certification/recertification of each accredited IS is kept current based on the DoDIIS Security Certification and Accreditation Guide. The accreditation security documentation package will be updated to reflect any changes and will be coordinated internally and forwarded to the appropriate SCO.

4.6.1 (U) Guest Systems in a SCIF

SCIFs are accredited under the authority of either DIA or NSA. Any system that enters the SCIF that has not already been certified or accredited by the respective cognizant SCIF authority is considered a Guest system. These guest systems may be brought into the SCIF only at the discretion of the cognizant authority and the local SSO/ISSM/ISSO as long as prudent IS Security measures and documentation are in place. An SSO is responsible for all resident SCI information, including that which exists on IS within a SCIF. The ISSM/ISSO supports the SSO in all security matters related to IS, and the DAA who accredits SCI systems within that SCIF is directly associated with the authority that established the SCIF, i.e., the cognizant DAA. Systems that process SCI under the cognizance of DIA and NSA have clear guidance as provided within this document. The following are three examples of guest systems:

- SCI or SAPI systems already certified by another PAA;
- SCI systems that have no existing certification; and
- Unclassified systems or systems with classification levels lower than SCI.

4.6.1.2 (U) SCI Systems with Certification

Within the DCID 6/3 community of PAAs, there is common acceptance of system accreditation and certification for systems that process SCI/SAPIs. These systems may be brought into a SCIF along with the certification documents provided by the PM/PMO so that the SCIF cognizant DAA may accredit the systems as they are connected to existing architectures. The ISSM will ensure that appropriate system documentation from the PM/PMO is available to the DAA/DAA Rep/SCO to support the accreditation prior to the system installation. If the guest systems will operate independently (not connecting to or

through existing architectures), the SSO/ISSM may accept the systems with accreditation as delivered and document the presence of these systems on configuration management architectures.

4.6.1.3 (U) SCI Systems without Certification

For SCI systems that do not have existing certification, the PM/PMO will provide appropriate documents for SCI Security certification and accreditation IAW Chapters 3 or 4.

4.6.1.4 (U) Unclassified or Collateral Systems

Non-SCI systems that are to be operated within a SCIF also require a certification/accreditation. These systems may be certified/accredited by an appropriate authority other than the cognizant SCI DAA. When the local Commander/SSO authorizes such systems to enter the SCIF and operate, then a coordinated policy/agreement should be established that addresses the security and operational interests of the different DAAs. The PM/PMO will deliver accreditation documentation for the systems to the SSO/ISSM with the request to install.

When a decision is made to allow GENSER or unclassified systems into a SCIF, a policy/agreement must be developed and documented by the SSO/ISSM. The SSO and ISSM are responsible for implementing appropriate security operating procedures before the respective systems/networks are permitted to enter the SCIF. These procedures will need to address IS security issues not already documented. The following are recommended issues to be included within the local procedures:

- Define the extent that the SSO/ISSM will have purview over the other DAA's systems while they are operated within the SCIF. This is an item that can be addressed in a MOA.
- Define the authority responsible for the respective systems and the SSO who retains oversight responsibility for SCI data within the SCIF.
- Document the coordination between SSO/ISSM in establishing the SCI controls for systems within a SCIF.
- Document TEMPEST countermeasures (e.g., update Fixed Facility Checklist and RED/BLACK separation compliance with Inspectable Space Determination).
- Develop an SOP for managing systems/media that are allowed to enter/depart the facility on a regular or recurring basis.

4.7 (U) MINIMUM SECURITY REQUIREMENTS

All DoDIIS systems and networks processing SCI will be protected according to DCID 6/3 by the continuous employment of appropriate administrative, environmental, and technical security measures. These measures will encompass individual accountability, access control, enforcement of least privilege, auditing, labeling, and data integrity.

4.7.1 (U) SSAA Content Classification

The minimum classification of a completed SSAA for DoDIIS information systems is CONFIDENTIAL.

4.8 (U) CERTIFICATION (IATO) AND ACCREDITATION (ATO) AUTHORITY

The following guidance is given and is depicted in table as Figure 4-1 below.

4.8.1 (U) Certification and Accreditation Authority for Protection Level 1 and 2

Certification and accreditation authority for Protection Level 1 and 2 information systems is delegated to the Service Certifying Offices (SCOs). Certification authority for Protection Level 1 and 2 information systems may be further delegated to Site Information Systems Security Managers (ISSMs) by the SCOs. SCO further delegation of authority shall be limited to systems or system baselines previously certified and/or accredited by a SCO, DIA, or other PAAs as identified in the DCID 6/3.

4.8.2 (U) Certification and Accreditation Authority for Protection Level 1, 2 and 3

Certification and accreditation authority for Protection Level 1, 2 and 3 information systems are hereby delegated to the Chief of the DIA Information Assurance Division (DIA/SYS-4).

- SYS-4A Certifiers are delegated certification (IATO) and accreditation authority (ATO) for PL 1 and 2. (Under normal circumstances, management [i.e., SYS-4 or SYS-4A] should sign all ATOs).
- SYS-4A Certifiers are delegated certification (IATO) authority PL 3.

4.8.3 (U) Certification Authority for Protection Level 4 and 5

Certification authority for Protection Level 4 and 5 information systems is hereby delegated to the DIA/SYS-4. Certification authority for Protection Level 3 and 4 information systems may be further delegated by DIA/SYS-4 to the SCOs on a case by case basis.

- SYS-4A Certifiers are delegated certification (IATO) authority for PL 4.

4.8.4 (U) Certification Authority for DoDIIS Site Baselines

Certification authority for DoDIIS Site Baselines is hereby delegated to the Chief of the DIA Information Assurance Division (DIA/SYS-4) and the SCOs.

- SYS-4A Certifiers are delegated certification (IATO) authority for Site Baselines.

4.8.5 (U) Accreditation Authority for Protection Level 4, 5 and DoDIIS Site Baselines

The DIRECTOR DIA, for Protection Level 4 and 5 information systems and DoDIIS Site Baselines, retains accreditation authority (ATO).

4.8.6 (U) Interim Approvals To Test (IATT)

All certifiers are authorized to grant Interim Approvals to Test (IATT). IATTs basically give authorization to test in a controlled environment only (e.g. test lab/controlled site) for a specified period of time, usually of a short duration. The IATT can be issued for testing in an operational environment for specific connection(s), data testing, etc.

	PL1		PL2		PL3		PL4		PL5		Site Base	
	IATO	**ATO**	**IATO**	**ATO**	**IATO**	**ATO**	**IATO**	**ATO**	**IATO**	**ATO**	**IATO**	**ATO**
DIR/DIA								**A**		**A**		**A**
Chief, SYS-4	**I**	**A**	**I**	**A**	**I**	**A**	**I**		**I**		**I**	
SYS-4	**I**	**A**	**I**	**A**	**I**		**I**				**I**	
SCO	**I**	**A**	**I**	**A**	**I***		**I***				**I**	
ISSM	**I***		**I***									

Figure 4-1: IATO/ATO Authority

- IATO = CERTIFICATION
- ATO = ACCREDITATION
- * ISSM – PL1 & PL2 certification authority can be delegated by the SCO.
- * SCO has certification authority for PL3 &PL4 ONLY as delegated by SYS-4 on a case-by-case basis.
- SYS-4 Note: Generally, all ATOs should go through management for signature, unless operational mission, TDY, etc., warrants immediacy.

CHAPTER 5 - TEMPEST

5.1 (U) PURPOSE

Information Systems (ISs), peripherals, associated data communications, and networks which may be used to process national security or security-related information may need to meet certain procurement and installation specifications as required by national TEMPEST policies and procedures applicable to the sensitivity level of the data being processed. This applies to all systems installed or planned. The objective of this area of security control is to minimize the risk of Hostile Intelligence Services (HOIS) exploiting unintentional emanations from intelligence systems. TEMPEST is a short name referring to investigations and studies of compromising emanations.

5.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

5.3 (U) DEFINITIONS

- Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements IAW National Security Telecommunications Information Systems Security Committee (NSTISSC)-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities (for example; DIA/DAC-2A).
- Compromising Emanations. Unintentional intelligence-bearing signals which if intercepted and analyzed disclose the national security information being transmitted, received, handled, or otherwise processed by any information processing equipment.
- Inspectable Space. The three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.
- Routine Changes. Changes that have a minimal effect on the overall TEMPEST security of the Sensitive Compartmented Information (SCI) Facility (SCIF). Adding a different type of electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment within the facility, and minor installation changes are examples of routine changes.
- Security Environment Changes. Changes that have a detrimental effect on the facility. Changes to the inspectable space, addition of a radio transmitter or a modem for external communications, removal or reduction of an existing TEMPEST countermeasure (Radio Frequency Interference [RFI] Shielding, Filters, Control/Inspectable space, etc.) would be changes to the security environment.

5.4 (U) TEMPEST COMPLIANCE

All facilities processing SCI will be reviewed by a CTTA for initial TEMPEST accreditation and/or Inspectable Space according to National Security Telecommunications Information Systems Security Policy (NSTISSP) 300, National Policy on Control of Compromising Emanations, and National Security Telecommunications and Information Systems Instruction (NSTISSI) 7000, TEMPEST Countermeasures for Facilities. The CTTA is authorized to make acceptable risk determinations for specific facilities when justified.

5.5 (U) ACCREDITATION

5.5.1 (U) TEMPEST Countermeasures Review

A CTTA must conduct or validate all TEMPEST countermeasure reviews. However, the requirement for a CTTA to conduct or validate such reviews does not imply the need to implement TEMPEST countermeasures. The recommended countermeasures will be threat driven and based on risk management principles. The inspectable space, as determined by a CTTA, will be the primary countermeasure.

5.5.2 (U) General Documentation

The local SCI security official will complete documentation IAW local TEMPEST Manager requirements. The local TEMPEST Manager will submit documentation IAW service directives. A record of the TEMPEST security accreditation or inspectable space determination (ISD) will be retained within the SCIF.

5.5.3 (U) TEMPEST/ISD Accreditation

When an inspectable site houses multiple IS facilities and has a relatively protected and uniform TEMPEST security environment, the CTTA may grant a TEMPEST site accreditation or ISD for electronic processing of SCI. Each SCIF within the inspectable site must be evaluated separately on its own merits and cannot be approved automatically by being inside an inspectable space. The accreditation/ISD could range from a building to a base/post if all space is inspectable. Compliance is reported within the SCIF Fixed Facility Checklist IAW DCID 6/9.

5.6 (U) TEMPEST INSTALLATION REQUIREMENTS:

- All computer equipment and peripherals must meet the requirements of National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92 and be installed IAW NSTISSAM TEMPEST/2-95, RED/BLACK separation criteria or as determined by a CTTA. The local TEMPEST Manager will oversee all such installations and coordinate on all accreditation documents resulting from the installation.
- Use all equipment as intended. All TEMPEST access doors, covers, and plates must be closed and fastened. Unauthorized modifications, even for testing purposes, are strictly forbidden.
- Additional TEMPEST requirements may exist if the equipment is not TEMPEST approved. In such a case, your local TEMPEST Manager should be contacted for further guidance.
- The local TEMPEST Manager must inspect all equipment installations.
- Special prohibitions and installation requirements exist for all transmitters, modems, and other networking and communications devices or equipment. Because of the broad range of this category, coordinate all requests for these devices with your local TEMPEST Manager.

- Do not consider a RED IS for any network which has any direct connection to a BLACK IS or other communications medium such as administrative telephone lines except through an approved cryptographic device.
- Do not use acoustically coupled modems and transmitters or locate them in any secure area without specific written approval from your DAA.
- You may use non-acoustic wire line modems with stand-alone, dedicated BLACK ISs providing that all appropriate telephone security requirements are met, consult with your local TEMPEST Manager.
- Wireless –Infrared (IR) and Radio Frequency (RF) systems. See Chapter 15 for discussion on restrictions for use within SCIFs.

CHAPTER 6 - MINIMUM SECURITY REQUIREMENTS FOR USERS

6.1 (U) PURPOSE

The purpose of this chapter is to identify the minimum-security requirements for a user of Information Systems. This chapter is designed so that it may be used as a general user reference for IS security training and awareness.

6.2 (U) SCOPE

This chapter identifies the minimum-security requirements for a general user necessary to operate an IS. These requirements are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

6.3 (U) MINIMUM SECURITY REQUIREMENTS

Users of ISs connected to networks shall use the system for official and appropriate use only. Personal use of a government IS must be approved by the user's supervisor IAW local policies.

6.3.1 (U) Identification and Authentication Requirements

Individual accountability is required for all users of IS that process SCI information. An IS user is identified through a unique USERID and a corresponding authenticator. The uniqueness of the USERID facilitates auditing and access controls. Group accounts (shared access through a single USERID) are prohibited unless the DAA approves this as an exception. An authenticator may be something the user knows, something the user possesses, or some physical characteristic about the user. The most common authenticator is a password. Users will comply with the following requirements to access IS:

- Users are required to login to all systems with an assigned USERID and password.
- Users are required to logout of all systems at the end of each workday or for an extended absence.
- Screen locks are mandatory, and require a password for reentry into the system. If an IS is idle for 15 minutes, the screen lock shall be activated automatically. Screen locks are not authorized in lieu of log-off procedures. Operations may require exceptions, which must be approved by the ISSPM/SCO.

6.3.2 (U) Password Requirements

The following policy will be used when issuing, controlling, and changing passwords:

- Passwords must be at least eight characters in length and consist of a mix of alphanumeric and special characters. .
- Only the user must know passwords.
- Users will not share their passwords with other users.

- Passwords will not be easily associated with an individual. Do not use words found in a dictionary. Do not use nicknames, spouse names, street names, vanity plate names, parts of the SSAN, telephone number, etc.
- All passwords must be protected at the same security classification as the accreditation level of the IS.
- A password must be changed if it has been compromised or has been in use for six months or less.
- Never write down passwords. Destroy the original password documentation following initial review. Never type passwords onto an IS when being observed by other people.
- Configure the minimum password age for at least 90 days, and the password history, which determines the number of unique new passwords that have to be associated with a user account before an old password can be reused, should have a minimum setting of five.
- Password evaluation tools may be used by sites for security assessment. Approval must be obtained through the ISSM.
- The following guidelines will be used when selecting a password:

DO:

- Include both upper and lower case characters.
- Include digits and punctuation marks.
- Include something that can be remembered without writing it down.
- Consider special-acronyms (e.g. N0tf#swvw - None of this fancy # stuff works very well).

DO NOT:

- Use any form of your logon name (e.g. initials).
- Use first, middle, last or maiden names.
- Use the name of a spouse, child, girl/boy friend.
- Use anything publicly available about you (e.g. address, car license plate number, car make, SSAN, etc.).
- Use all the same type of characters (e.g. 123245678, AAAAAAAA, etc.).
- Use a word or words from a dictionary.
- Use substitution of characters by switching ones (1) for “ells” (l) or zeros (0) for “ohs” (o).
- Use names or characters from fantasy and science fiction stories (Quagmire, etc.).

6.3.3 (U) IS Warning Banner

All systems are required to display a logon warning banner. When the user logs on to a system, the user agrees to accept the conditions of the warning. The following applies:

- A logon warning banner is required on all networked and standalone DoD interest computer systems (Government and contractor).
- The warning banner must be displayed before a successful logon and should include an option that allows the user to halt the logon process and a keystroke to continue processing. The intent of the

banner is to confirm to the user that all data contained on DoD interest computer systems is subject to review by law enforcement authorities, DoD security personnel, and/or System Administrator, IAW Chapter 9. The banner is designed to inform all users, prior to accessing a DoD system, that by logging in they expressly consent to authorized monitoring.

- ISs supporting DoD operations have very specific warning banner requirements, and must include, at a minimum, the information shown in Figure 9.1.
- Whenever system administration personnel suspect that a system is being inappropriately used, either by authorized or unauthorized personnel, or some improper activity is being conducted, the matter will be reported immediately to the ISSO/ISSM. Refer to Chapter 8 for additional guidance.

6.3.4 (U) Configuration Management Requirements

The following policy will be used for the CM of all systems.

- Modifying, relocating, or reconfiguring the hardware of any computer system must be approved by the CCB or the CMB for each site. Hardware will not be connected to any system/network without the express written consent of the ISS0/ISSM and the CMB/CCB. ’
- Modifying, installing, or downloading of any software on any computer system may affect system accreditation and must be evaluated and approved by the ISSO/ISSM with the local CMB/CCB.

6.3.4.1 (U) Authorized Software

Software that may be authorized includes that which has been:

- Provided officially by another U.S. Government Agency that has equivalent standards.
- Provided under contract to organizations involved with the processing of SCI and related intelligence information.
- Developed within a Government-approved facility.
- Provided through appropriate procurement channels, i.e. COTS software.
- Distributed through official channels.

6.3.4.2 (U) Unauthorized Software

Types of software that are not authorized include:

- Games (See paragraph 11.6.).
- Public domain software or “shareware” which have been obtained from unofficial channels.
- Software applications that have been developed outside Government approved facilities, such as those developed on personally owned computers at home or software acquired via non-U.S. Government “bulletin boards”.
- Personally owned software (either purchased or gratuitously acquired).
- Software purchased using employee funds (from an activity such as a coffee fund).
- Software from unknown sources.
- Illegally copied software in violation of copyright rules.
- Music and video or multimedia compact disks, not procured through official Government channels.

6.3.5 (U) Malicious Code Detection

Users of IS play a very important role in the prevention of malicious codes. For details, see Chapter 10. To actively participate in the prevention of malicious codes on an IS, users must be made aware of, and comply with, basic security requirements. Warnings and advisories frequently provide guidance on preventing infection from malicious code or viruses—obey these. If a malicious code is detected or a presence of malicious code is suspected on any IS, immediately report it to the ISSO/ISSM IAW Chapter 8. Do nothing that might cause the further spread of the malicious code.

6.3.6 (U) Malicious Code Prevention

The user is responsible for ensuring that the following procedures are followed to minimize the risk of malicious code:

- Will not import or use unauthorized data, media, software, firmware, or hardware on systems.
- Use automated virus scanning applications on all media prior to use. If the media cannot be scanned then it is considered high risk and cannot be used on any IS without approval from the SCO.
- Avoid hostile mobile code through use of only authorized/verified and registered mobile code.
- Will not knowingly or willfully introduce malicious code into systems.
- Will conduct screening of all incoming data (e.g., E-Mail and attachments) if this process is not automated.
- Will not use personally owned media (e.g., music, video, or multimedia compact disks) in Government-owned IS.
- Will immediately report all security incidents and potential threats and vulnerabilities involving malicious code on ISs to the ISSO/ISSM.

Note: Controlled Interfaces with malicious code scanning capability do not relieve the management of the receiving IS from the responsibility of also checking for malicious code.

6.3.7 (U) Removable Information Storage Media

Removable information storage media with an IS will have external labels clearly indicating the classification of the information and applicable associated markings (e.g., digraphs, trigraphs). Examples include magnetic tape reels, cartridges, cassettes; removable discs, disc cartridges, disc packs, diskettes, magnetic cards and electro-optical (e.g., CD) media. Labeling exemption for operational security (OPSEC) requirements may be granted within local policy with DAA/DAA Rep concurrence. All removable information storage media will be marked with the appropriate Standard Form (SF) 700-series classification and descriptor labels (See Chapter 12 for a visual depiction of each). These are:

- SF 706, Top Secret Label
- SF 707, Secret Label
- SF 708, Confidential Label
- SF 710, Unclassified Label
- SF 711, Data Descriptor (On all magnetic media)
- SF 712, Classified SCI Label (All classification levels)

6.3.7.1 (U) Label Placement

Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media. Labels for Compact Disks (CDs) must NOT be placed on the CD itself, but on the CD container or envelope. Record the accounting number in the "Control" block of the SF 711 and write the same number on the CD with a Paint-pen, CD label maker or permanent marker. The number should not interfere with the operation of the CD. Notice: Do not use pens that contain toluene.

6.3.7.2 (U) Data Descriptor Label

The SF 711, Data Descriptor Label, is used to identify the content of a specific media to include unclassified, collateral-classified, and SCI. A SF 711 is not required if the disk bears the following information: Organization, office symbol, classification, and media sequence number (if locally required). The user fills in the "Classification", "Dissem", "Control", and "Compartments/Codewords" blocks as appropriate.

6.3.7.3 (U) Classification Markings

All documents residing or processed on information storage media/ISs will be marked IAW DCID 6/3, Controlled Access Program Coordination Office (CAPCO) guidance "Intelligence Community Classification and Control Markings Implementation Manual", dated 10 Sep 1999 (Amended 21 March 2002), DoD 5105.21-M-1, dated August 1998, or appropriate Agency/Service regulations.

6.3.7.4 (U) Control and Accounting of Media

For any system that operates with PL-3 or lower functionality, media that is not write-protected and is placed into that system must be classified at the highest level of information on the system until reviewed and validated. Media accountability will be based on the determined classification level of the media.

6.3.7.4.1 (U) Information Storage Media Control

In addition to the labeling of information storage media according to Chapter 12, there is a requirement to control and account for certain information storage media within functional categories. The organization Commander/CO/SIO is responsible for development of a unit-level Standard Operating Procedure (SOP) for control and accountability of media.

6.3.7.4.2 (U) Inspections

The organization must be able to demonstrate positive control and accounting of information storage media according to its SOP when reviewed by inspection authorities.

6.3.7.4.3 (U) Control Procedures

Control of information storage media should begin upon introduction into the organization according to the SOP.

- (U) Information storage media accountability is required for Top Secret BRAVO and permanent Collateral Top Secret files.
- (U) Information storage accountability as a security protection measure is eliminated for collateral classified information (to include Top Secret non-permanent files), all classification levels of Special Intelligence (SI) (to include GAMMA and ENDSEAL), Talent-Keyhole (TK), and BRAVO material below Top Secret.

- (U) The respective Program Manager will define requirements for controls of specific Special Access Program (SAP) information.

6.3.7.4.4 (U) Other Categories of Storage Media

The following major categories of information storage media should be considered for accountability control in compliance with copyright and licensing with procedures documented in the SOP:

- COTS and vendor software.
- Government developed software.
- Other organization unique software and data.

6.3.8 (U) Hardware Labeling Requirements

Labels will be displayed on all components of an IS. This includes input/output devices that have the potential for retaining information, terminals, standalone microprocessors, and word processors used as terminals, bear conspicuous external labels stating the highest classification level and most restrictive classification category of the information accessible to the components in the IS. The labels should be the standard form (SF) 700 series media classification labels or equivalent (see Chapter 12). The labeling may consist of permanent markings on the component or a sign placed on the terminal.

6.3.9 (U) Security Training Requirements

An integral part of the IS security program is the mandatory training required by public law. Users will receive initial training on prescribed IS security restrictions and safeguards prior to accessing corporate IS assets. General users require system security training to safeguard systems and information on those systems/networks, contact the local ISSM. As a follow-up to this initial training, users must be provided, and actively participate in an ongoing security education, training, and awareness program which will keep them cognizant of system changes and associated security requirements as they occur. General users training will include but is not limited to the following:

- An awareness of system threats, vulnerabilities, risks, system data, and access controls associated with the IS being used.
- How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).
- How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by user).
- How to recognize and report security violations and incidents see Chapter 8.

6.3.9.1 (U) Security Awareness and Training Program

The key to protecting Information Systems (ISs) & Networks and the information they process is the development of an effective Security, Education, Training and Awareness Program. The program is intended to provide two levels of knowledge:

6.3.9.1.1 (U) Awareness Level

Creates sensitivity to the threats and vulnerabilities of national security information systems, and recognition of the need to protect data, information and the means of processing them; and builds a

working knowledge of principles and procedures in IA. Awareness level training will be conducted when:

- In-processing. Site specific information will be briefed based on the mission and the requirement of the job responsibility.
- Receipt of USERID and Password. Privilege User/ISSO will brief the user on his/her responsibilities.
- Annual Awareness Refresher Training. Classroom, Briefings, Computer Based Training, or Seminars will be used and documented to ensure all users comply with this requirement.

6.3.9.1.2 (U) Performance Level

Provides the employee with the skill or ability to design, execute, or evaluate agency IA security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

6.3.9.1.3 (U) General Users training

General users training will include but is not limited to the following:

- How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).
- How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by user).
- How to recognize and report security violations and incidents.
- The organization's policy for protecting information and systems.

6.3.10 (U) Destruction of Media

When destruction of information storage media is required, it must be accomplished IAW approved procedures and the organization's media accounting system must be updated to reflect this change. See Chapter 21, Paragraph 21.5.4 Destroying Media, for additional guidance.

- (U) Destruction certificates are required for accountable material and will be retained as a permanent record.
- (U) Non-accountable material no longer requires destruction certificates.

6.3.11 (U) Information Transfer and Accounting Procedures

Users should be knowledgeable of procedures for the transfer of information or software among ISs of different classification levels using information storage media. Contact the ISSM for local procedures. The procedures are intended to protect the confidentiality of information on the media as well as other data on the end-point IS at different levels, prevent transfers of malicious code (Chapter 10 is germane), and prevent violation of legal copyright or license rights. For any system that operates with PL-3 and below functionality, media that is placed into that system must be classified at the highest level of information on the system until reviewed and validated. See Chapter 18.

CHAPTER 7 - SECURITY GUIDELINES FOR THE PRIVILEGED USER

7.1 (U) PURPOSE

The Privileged User is assigned by management personnel (at NSA/CSS the Office of Security approves Privileged User) and is the single point of contact for the administration of a specifically defined Information System (IS). The privileged user is responsible for maintaining the IS throughout day-to-day operations, ensuring that the system operates within established accreditation criteria, and keeping the system in an operational mode for general users. System administration personnel are the primary interface between the users of an IS and the organization's Information Systems Security (ISS) management personnel. This chapter provides the privileged user with the security guidance and procedures necessary to implement an effective System Administration program.

7.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

7.3 (U) SECURITY TRAINING

The individual assigned the responsibility for IS administration must be knowledgeable in the basic security concepts and procedures necessary to effectively monitor IS activity and the environment in which it operates. Contact the ISSM for applicable training.

7.3.1 (U) Privileged User training

Privileged user training will include but is not limited to the following:

- How to protect the physical area, media, and equipment (e.g. locking doors, care of diskettes, etc.)
- Understand security consequences and costs so that security can be factored into their decisions.
- Have a thorough understanding of the organization's policy for protecting information and systems, and the roles and responsibilities of various organizational units with which they may have to interact.
- Have a thorough understanding of system security regulations and policies.
- Be aware of what constitutes misuse or abuse of system privileges.
- Have an understanding of how to protect passwords, or other authentication devices, and be familiar with operating system security features of the system.
- Know how to recognize and report potential security vulnerabilities, threats, security violations, or incidents.
- Understand how to implement and use specific access control products.

- Have an understanding of how to protect the media and equipment (e.g. system maintenance and backup, care of diskettes).
- How to protect authenticators and operate the applicable system security features.

7.3.2 (U) Security Awareness and Training Program

The key to protecting ISs and networks and the information they process is the development of an effective Security, Education, Training and Awareness Program. The program is intended to provide two levels of knowledge:

7.3.2.1 (U) Awareness Level

Creates sensitivity to the threats and vulnerabilities of national security information systems, and recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and procedures in IA. Awareness level training will be conducted when:

- Inprocessing. Site specific information will be briefed based on the mission and the requirement of the job responsibility.
- Receipt of USERID and Password. Privilege User/ISSO will brief the user on his/her responsibilities.
- Annual Awareness Refresher Training. Classroom, Briefings, Computer Based Training, or Seminars will be used and documented to ensure all users comply with this requirement.

7.3.3.2 (U) Performance Level

Provides the employee with the skill or ability to design, execute, or evaluate agency IA security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

7.4 (U) LEAST PRIVILEGE IMPLEMENTATION

Because system administration personnel do not always have to perform functions using their fully privileged account, therefore they should maintain a separate general user account.

7.5 (U) SCI SYSTEM SECURITY PROCEDURES

SCI IA doctrine requires many security relevant actions to properly implement a secure environment to protect national interest information. The following procedures outline several items that apply to all SCI ISs and must be given full consideration by system administration personnel.

7.5.1 (U) Identification and Authentication Requirements

USERIDs are used for identification of a specific user on the IS to facilitate auditing. Group accounts are generally prohibited; exceptions to this policy shall be approved by the DAA/DAA Rep. Passwords (as authenticators) are used to provide an access path for authorized users while denying access to the unauthorized user. Use the following procedures to generate issue and control USERIDs and passwords.

7.5.1.1 (U) Documenting USERIDs and Passwords

Document the issuing of USERIDs and passwords IAW established DAA requirements and local procedures.

7.5.1.2. (U) USERID and Password Issuing Authority and Accountability

The ISSM or designee is the official authorized to issue the initial USERID and password to each user of the system. The ISSM or designee will maintain a current user account roster for each system for which they are responsible, to include the names of authorized maintenance personnel. The roster will contain, at a minimum, each user's:

- Never enter the assigned password of an individual on a form used to establish a user's account. The issuing ISSM/SA will distribute the initial password in a secure manner. The requesting individual must authenticate that a password has been received, and the signed form must be returned to the ISSM/SA before activation of the account. The form will be retained by the ISSM/SA for a minimum of one year after access is removed.
- Full name, grade or rank, and Social Security Account Number (SSAN).
- Organization, office symbol, and telephone number.
- USERID.

7.5.1.3 (U) Supervisor Authorization

Obtaining supervisor approval for each individual requiring IS access. The privileged user must ensure that all individual access authorizations are valid, need-to-know is established and access is work-related.

7.5.1.4 (U) Access Requirements Validation

The privileged user will provide each functional area within the organization with a current general user roster (for that functional area only) and require that the supervisor validate all access requirements annually at a minimum. The annual validation process will be documented.

7.5.1.5 (U) Account Management

A user account will be deactivated when that account is idle for an extended period (recommend 60 days). The loss of security clearance requires immediate deactivation of the account.

7.5.1.6 (U) Tactical/Deployable Use of group accounts

As group accounts are generally prohibited; exceptions to this policy are as follows:

- Security requirement: Individual accountability for all users requires individual accounts which can be monitored through automated audit capabilities (see DCID 6/3).
- Operational requirement: Use of group user accounts in a tactical/watchstanding environment allows rapid interchange between users whose primary focus is quick access to the system without interruption of functions or capabilities. This also avoids system transients (and potential for errors on startup) as the system is shut down and restarted for a different user to logon.
- Sample security implementation: Lists do exist for watchstander rotations or battle station assignments, which could be retained and used to augment activity logs to correlate user identities to actions as recorded on audit logs. Advanced alternative: Developers provide a simple pop-up "change USERID" GUI which does not cause the system to shutdown or change operations, but which simply changes accountability via the new USERID/password for continuing processes for an individual member of a common functional group.

7.5.2 (U) System Access and Removal Procedures

Access and removals from an IS must be documented IAW local procedures.

7.5.3 (U) Audit Trail Requirements

An audit trail capability must exist to obtain formal accreditation of an IS. The audit trail should be automated, and provide permanent on-line or off-line storage of audit data separate from data files. Audit reduction tools are highly recommended and are endorsed by DCID 6/3 paragraph 4.B.2.a(6), Audit3. Although there are no specific audit reduction tools recommended, tools such as PReCis and TNE (Trusted Network Environment) are the type of auditing tools available.

7.5.3.1 (U) Automated Audit Trail Information Requirements

ISs approved for classified processing should contain, at a minimum, the following audit trail records:

- Login (Success, Failure) Logout (Success).
    - Auditing of successful login and logout events is key to individual accountability. Unsuccessful login attempts may be evidence of attempted penetration attacks. Logins and logouts shall be audited by the underlying operating system. In addition, the syslog mechanism may be used to notify an ISSM/SA of an unsuccessful login attempt.
    - Audit data should include date, time, USERID, system ID, workstation ID, and indication of success or failure.
- Use of privileged commands. (Failure)
    - Privileged commands are commands not required for general use, such as those that manage security-relevant data and those that manage an application. In UNIX workstations, these commands include, for example, the SU command, which is used to become the root user. The UNIX root user has access to all information stored on the system. Such commands must be accessible only to persons whose responsibilities require their use.
    - The ISSM/SA shall select the privileged commands (i.e., commands normally executed by the root user) to be audited. This event can be audited via the underlying operating system or application audit.
    - Audit data should include date, time, USERID, command, security-relevant command parameters, and indication of success or failure.
- Application and session initiation. (Failure)
    - The use of application programs and the initiation of communications sessions with local or remote hosts are audited to provide the ISSM/SA a general history of a user's actions. An unsuccessful attempt to use an application or initiate a host session may indicate a user attempting to exceed his or her access authorizations. This event should be audited via application audit.
    - Audit data should include date, time, USERID, workstation ID, application ID, and indication of success or failure.
- Use of print command. (Success)
    - The printing of classified and sensitive unclassified information is audited to maintain accountability for these materials. Print commands and the identity of the printed material should be audited via application audit.

  - Audit data should include date, time, USERID, and destination.

- Discretionary Access Control (DAC) permission modification. (Success, Failure)
  - The changing of DAC permissions on files or directories should be audited since it could result in violations of need-to-know. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, user (requester) ID, user/group ID (to whom change applies), object ID, permissions requested, and indication of success or failure.
- Export to media. (Success).
  - The copying of files to removable media should be audited to maintain accountability of classified materials. Removable storage media have large capacity and could potentially disclose large amounts of information. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, USERID, source and destination file IDs, system ID, and device ID.
- Unauthorized access attempts to files. (Failure)
  - An attempt to access files in violation of DAC permissions could indicate user browsing and must be audited. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, USERID, system ID, and file ID.
- System startup/shutdown. (Success, Failure)
  - System startup and shutdown shall be monitored and be auditable. This event should be audited by the operating system.
  - Audit data should include date, time, USERID, system ID, and device ID.

7.5.3.2 (U) Manual Audit Trail Implementation

If Automated Audit Trails are not supported, the ISSM/SA must obtain approval from the ISSPM/SCO to conduct manual audits. At a minimum, manual audits will include:

- The date.
- Identification of the user.
- Time the user logs on and off the system.
- Function(s) performed.

7.5.3.3 (U) Products of Audit Trail Information

Audit trail products should be handled as follows:

- Classify and protect audit trail information according to the security classification level of information contained in the audit.
- If hardcopy audit trail products are generated on an IS, print them on continuous paper whenever possible. If continuous paper is not used, all pages will be numbered with a sequence number on each printed line. This is required to protect the integrity of the audit trail data.

- Where possible, to reduce workload, generate summary reports which reflect system abnormalities, who performed what function, and to what database, rather than listing the entire audit trail.

7.5.3.4 (U) Audit Trail Checks and Reviews

The ISSO/SA will review the audit trail logs (manual and automated), or summary reports, to verify that all pertinent activity is properly recorded and appropriate action has been taken to correct and report any identified problems. Paragraphs 7.5.3.1 and 7.5.3.2 list audit trail requirements. Audit trail logs or summary reports shall be reviewed weekly, at a minimum, or as directed by the ISSM.

7.5.3.5 (U) Audit Trail Records Retention

Retain Audit Trail records for five years.

7.5.3.6 (U) Tactical/Deployable Audit Process Requirements

ISs which process SCI data may be developed specifically for tactical environments and are implemented with tactical/deployable features that are contrary to SCI security requirements. The following audit requirements should be viewed from a mission impact and adhered to accordingly.

- Security requirement: If the Audit process fails, the system is unable to provide monitoring for unauthorized activities and should not continue operating, but should default to a safe/secure posture pending restoring the ability to maintain proper audit.
- Mission Critical requirement: Failure of the Audit process should not interfere with continued normal operation of a system.
- Sample implementation: Allow the system to continue operation if the Audit process fails.

7.5.3.6.1 (U) Tactical/Deployable Audit log requirements

- Security requirement: If the Audit logs fill up and the system is unable to record the monitoring information for unauthorized activities, it should not continue operating, but should default to a safe/secure posture pending proper retrieval/storage/archive of the audit data.
- Operational requirement: Full audit logs should not interfere with normal operation of a system. Audits may fill up due to other than normal activities required to support operations, or a system administrator being too busy responding to another operational requirement.
- Sample security implementation: Placing operational requirements ahead of security requirements could result in the Audit process being set for “overwrite oldest if full” or First-In-First-Out (FIFO) overwrite.

7.5.4 (U) Automatic Log-Out Requirements

The privileged user should implement an automatic logout from the IS when the user leaves his/her terminal for an extended period of time. This should not be considered a substitute for a user logging out.

7.5.5 (U) Limited Access Attempts

An IS will be configured to limit the number of consecutive failed access attempts to no more than five; three is recommended.

7.5.6 (U) Use of Windows Screen Locks

Screen locks are mandatory, and require a password for reentry into the system. If an IS is idle for 15 minutes, the screen lock will be automatically activated. Screen locks are not authorized in lieu of log-off procedures. Operations may require exceptions which must be approved by the ISSPM/SCO.

7.5.6.1 (U) Tactical/Deployable Protection for Information against unattended operation

- Security requirement: When a terminal is not attended, screen savers, screen locks, and dead man lockout features provide protection of classified information. These features can interrupt an operation when a terminal is left in a monitoring mode while other evolutions are taking place.
- Operational requirement: Long term monitoring may be required without continuous user interaction with a system. Rapid response may require eliminating delays resulting from required security passwords on screen locks. The need for rapid response could also completely obviate dead man timeout features.
- Sample security implementation: disable these features for the IS for use in the tactical environments.

7.5.7 (U) Testing, Straining, and Hacking

SCI IA policy states that testing, straining, hacking, or otherwise attempting to defeat or circumvent the security measures of an operational IS or network is prohibited without authorization. The privileged user must ensure that submitting a request through the ISSM to the DAA Rep/SCO approves such activities. All such approvals must be in writing and limited to an explicit assessment.

7.5.8 (U) Warning Banners

A logon warning banner is required on all networked and standalone DoD computer systems (Government and contractor). The warning banner must be displayed and acknowledged before a successful logon. Refer to Chapter 9 for complete instructions on the implementation of warning banners.

7.5.9 (U) Network Monitoring

7.5.9.1 (U) Maintenance Monitoring

Privileged users/network technicians may use Local Area Network (LAN) analyzers or “sniffers” to monitor network traffic provided:

- Reasonable notice has been provided to all users by display of the warning banners (Paragraph 9.3.1).
- The base or post has been certified for monitoring by the Service General Counsel (if required by the appropriate Service).
- The sniffer or monitor does not intercept any traffic from outside the military base or post.
- The privileged user has received approval from the ISSM/ISSPM to monitor in the normal course of his or her employment while engaged in activity necessary incident to the rendition of his or her service or to the protection of the rights or property of the communications network (the provider of the network service) except that this monitoring is only permitted for service or mechanical quality control checks.

- Network traffic monitoring may not last longer than is necessary to observe transmission quality.
- No permanent recording of the network monitoring activity may be made.
- Monitoring traffic on civilian networks is strictly prohibited and may result in criminal and civil liability under the Computer Fraud and Abuse Act, 18 U.S. Code section 1030 and the Electronic Communications Privacy Act, 18 U.S. Code Section 2510 and following.

7.5.9.2 (U) Targeted Monitoring

Unauthorized targeted monitoring of a particular individual, machine or group is prohibited. When service quality or transmission quality monitoring reveals suspicious activity, including hacking or misuse, monitoring must cease and appropriate officials informed. At a minimum, notify the Commander/Commanding Officer, or his/her designated representative, and the ISSM. Privileged users may, of course, always terminate any connection at any time when the safety or property of the network is endangered. Privileged users shall cooperate with law enforcement and security officials IAW applicable Service guidelines.

CHAPTER 8 - INFORMATION SYSTEMS (IS) INCIDENT REPORTING

8.1 (U) PURPOSE

Incidents may result from accidental or deliberate actions on the part of a user or occur outside of the organization as well. An accidental incident should be handled administratively. Evidence of criminal activity from a deliberate action should be treated with care, and maintained under the purview of cognizant law enforcement personnel (see Chapter 9 "Information System Monitoring Activities" for specific guidance). All management personnel must ensure IS users are aware of the policy governing unauthorized use of computer resources. When it is suspected that an IS has been penetrated, or at any time system security is not maintained, it must be reported both within the organization and to the appropriate external authorities for action. Any use for other than authorized purposes violates security policy, and may result in disciplinary action under the Uniform Code of Military Justice (UCMJ) and/or other administrative directives. This chapter provides procedures for formal incident reporting.

8.2 (U) SCOPE

These procedures are effective in the following life-cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

8.3 (U) PROCEDURES

Discovery of a viral infection, introduction of malicious code, hacker activity, system vulnerabilities, or any unusual happenings will be reported immediately to the ISSM and an investigation initiated. Accidental incidents (for example, a one time brief Web site visit containing inappropriate content or inappropriate or vulgar usage of mission systems chat features) or other minor infractions can be handled administratively within the unit. Make every effort to contact the data owner to obtain specific guidance to afford minimum acceptable protection in cases of spillage and compromise.

8.3.1 (U) Reporting Process

Incident reporting should be accomplished by each service through their appropriate ISSM or security channel.

8.3.2 (U) Types of IS Incidents and Reports

The following are examples of incidents that must be reported:

- Data Compromise. Is the compromise or probable compromise of classified information resulting from the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), computer generated output; human error in reviewing media for content and classification resulting in compromise; and incorrect setting of a security filter resulting in compromise.
- Spillage. Information of a higher classification or restrictive in nature intentionally or inadvertently placed on machines or networks of lower classification or less restrictive policy.

- External Hacker Activity. Activity where a hacker is operating from an outside location by using some network and he/she is not physically resident at the location where the activity is being observed.
- Internal Hacker Activity. Activity where a hacker is operating from within the site where the activity is being observed.
- Malicious Code. Any potentially hazardous or destructive computer code other than a virus, such as a logic bomb, worm or Trojan horse. NOTE: malicious code will probably also represent a vulnerability, as described below.
- Unauthorized Monitoring. Any individual or group of individuals found to be monitoring an IS without written authority from security officials.
- Unauthorized Software. Software obtained through unofficial channels see paragraph 11.6.4.
- Virus Actual Infection. A known active attack or presence on an IS where the virus has executed on that system.
- Vulnerability. Any detected lack of protection that may render the system vulnerable to security breaches. Examples are failure, or potential failure, of a system or network security feature. The discovery of any computer code, such as a trapdoor, which was originally coded into the operating system by the software vendor; or code added by software maintenance personnel, that provides an undocumented entry/exit capability into the system by unauthorized personnel.

8.3.3 (U) Reporting Incidents

Incidents in progress are classified a minimum of CONFIDENTIAL IAW NSA/CSS Classification Guide 75-98 or DoD 5105.21-M-1. The cognizant intelligence agency (DIA or NSA) should be notified via secure channels by electrical message (AUTODIN), E-Mail or agency web site as soon as the unit has knowledge of an incident or specifics. The notification should contain the information in paragraph 8.3.4. (see Figure 8.1 for an example of an AUTODIN message). Initial/interim reporting should begin as soon as possible after knowledge of the incident but should continue until the incident is resolved. Remember to include information copies of the report to the DAA Rep/SCO and chain of command (for example, AIA, INSCOM, SSO NAVY, CNSG). Complete the report according to the format in paragraph 8.3.4 below and send to the appropriate Service addressees.

- SCEs will report to the Security Health Officer (SHO) desk in the NSA/CSS Information System Incident Response Team (NISIRT), phone: DSN 644-6988/Commercial (301) 688-6988.
- DoDIIS sites will report to the DIA ADP Command Center, phone: DSN 428-8000/Commercial (202) 231-8000. For guest systems, reporting should be to both the cognizant SCIF authority and the guest system DAA Rep/SCO.

Caution: If a hacker is suspected of monitoring the Automatic Digital Network (AUTODIN)/Defense Message Messaging System (DMS) message traffic, do not use AUTODIN/DMS to send the report. Instead, send the report by facsimile to the required addressees, followed up by a phone call to confirm receipt of the report.

Users playing games on the systems, or fraud waste and abuse issues are incidents and should be reported and dealt with by the unit’s chain of command.

8.3.4 (U) Report Format and Content

When reporting incidents, include the following information in the body of the message (as shown in sample message, Figure 8.1):

- Type of Incident. Enter the type of incident report directly from paragraph 8.3.2 above. If there is any doubt when choosing the "type" of incident, identify the incident as both (or multiple) types in the same message. Selecting the most appropriate incident type is not nearly as important as reporting the incident.
- Date and Time the Incident Occurred. Enter the date and time that the occurrence was first detected.
- Name and Classification of the Subject IS. Enter the name of the system identified in the accreditation documentation, a current description of the hardware and software on the system, and the highest classification of information processed.
- Description of the Incident. Clearly describe the incident in detail.
- Impact of the Incident on Organization Operations. This is usually stated in terms of "denial of service", such as having to isolate the IS from a network, thereby closing down operations, etc. Include the number of hours of system downtime and how many man-hours needed to correct the problem.
- Impact of the Incident on National Security. Per DoD 5105.21-M-1, when classified information has been released to unauthorized persons, you must treat the incident as a security violation. List the name of the SCI security official to whom you have reported the incident.
- Man-hours involved in recovery, cleanup, etc. This provides an accurate metric to track incident recovery man-hours and resources involved. Tracking can include cost estimates related to the hours/wage grade spent.
- Point of Contact (POC). Enter the name, rank, organization, office, and telephone number of the person to be contacted on all subsequent actions concerning this incident.

-

R 211234Z FEB 01

FM *YOUR UNIT*//OFFICE//

TO SSO DIA//SYS-4/DAC-3D//

NSACSS//SHO/L1//

INFO *CHAIN OF COMMAND*

***SCO*//OFFICE//**

ZEM

C O N F I D E N T I A L

QQQQ

SUBJECT: INCIDENT REPORT ICW JDCSISSS, CHAPTER 8

1. TYPE OF INCIDENT: (VIRUS, MALICIOUS CODE, DATA COMPROMISE, SUSPECTED PROBLEM)

2. DATE/TIME INCIDENT OCCURRED

3. NAME AND CLASSIFICATION OF VICTIMIZED SYSTEM

4. DESCRIPTION OF INCIDENT: (AS MUCH DETAIL AS NECESSARY TO ADEQUATELY DESCRIBE THE PROBLEM)

5. IMPACT OF INCIDENT ON ORGANIZATION OPERATIONS (USUALLY STATED IN TERMS OF DENIAL OF SERVICE, DOWN TIME OR MISSION IMPACT)

6. IMPACT OF THE INCIDENT ON NATIONAL SECURITY (USUALLY STATED IN TERMS OF DATA OWNER'S ASSESSMENT OF LEVEL OF CLASSIFIED INFORMATION AND COMPROMISE PROBABILITY)

7. MAN-HOURS REQUIRED TO COMPLETE RECOVERY

8. ACTIONS TAKEN TO RECOVER

9. REPORTING UNIT POC (NAME, RANK, ORG/OFFICE, PHONE NUMBERS, E-MAIL ADDRESS)

NNNN

Figure 8.1 (U) Sample Incident Report Message

8.3.5 (U) Follow-On Action

Units will continue to report until the incident is closed. Virus infections that are corrected should be reported as "closed", unless further actions are being taken, or reinfection has occurred. The HQ-level action addressees and Data Owners will determine follow-on actions. Appropriate PAA/designee will determine course of action for incident cleanup in a near real-time manner. Once an incident has been resolved (i.e., closed), the incident may be treated as FOUO. The DAA Rep/SCO will coordinate with the DIA or NISIRT to ensure that the concerns of the latter are addressed. If an activity from another command or agency is involved, the HQ-level action addressees will provide proper notification to the same.

CHAPTER 9 - INFORMATION SYSTEM (IS) MONITORING ACTIVITIES

9.1 (U) PURPOSE

This chapter provides guidance on the DOs and DON'Ts of IS monitoring and applies to all computer systems and networks. All U.S. Government systems must be protected from intrusion and exploitation. Therefore, it is mandatory this guidance is implemented. Intrusions may result in denial of service, misuse, destruction and modification of data or programs, and disclosure of information. Typically, the personnel and physical security disciplines add credence to the protection afforded Government systems, especially those that are classified. Occasionally, when the incident requires further action, some monitoring must be established as an additional tool to protect the critical system and to identify the perpetrator attempting to violate the security of the system.

9.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

9.3 (U) PROCEDURES

In the DoD environment, the policy is to protect classified and unclassified sensitive information from unauthorized disclosure, destruction and modification. The security policies have been constructed to meet this objective. Implementation of these security policies begins with a warning to the user that the system is subject to monitoring. Once this has been done, the user acknowledges that monitoring may be initiated when appropriately authorized and determined necessary to provide documentary evidence for a potential prosecution or administrative action. Extreme care must be taken in a targeted monitoring situation, IAW this chapter, to ensure:

- Evidence is not destroyed.
- Innocent personnel are not implicated.
- The subject does not become aware of a planned monitoring activity.

9.3.1 (U) IS Warning Banner

The DoD General Counsel requires explicit notice to all users that use of Information Systems constitutes consent to monitoring. User knowledge of monitoring activation can serve as a deterrent to any malicious act. The following warning banner requirements are to be applied

- (U) A logon warning banner is required on all networked and standalone DoD interest computer systems (Government and contractor). The warning banner must be displayed before a successful logon and should include an option that allows the user to halt the logon process. The intent of the banner is to confirm to the user that all data contained on DoD interest computer systems is subject to review by law enforcement authorities, DoD security personnel, and/or System Administrator,

IAW this chapter. The banner is designed to inform all users, prior to accessing a DoD system, that by logging on they expressly consent to authorized monitoring.

- (U) ISs supporting DoD operations have very specific warning banner requirements, and must include, at a minimum, the information shown in Figure 9.1.
- (U) A warning banner must be placed on an IS so that the IS user must enter a keystroke to continue processing. Although an appropriate warning banner is displayed, systems administration personnel will minimize the possibility of accessing user data that is not relevant to the monitoring being acquired, analyzed, or recorded. Whenever system administration personnel suspect that a system is being inappropriately used, either by authorized or unauthorized personnel, or some improper activity is being conducted, the matter will be reported immediately to the ISSM/ISSPM.

NOTICE AND CONSENT BANNER

THIS IS A DEPARTMENT OF DEFENSE (DOD) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Figure 9.1. (U) Information System Warning Banner.

9.3.2 (U) Warning Labels

In addition to the IS warning banner, a standard U.S. Government warning label must be placed on the top border edge of each terminal of each IS. Local production of labels is authorized only when using the text contained in Figure 9.2.

THIS INFORMATION SYSTEM (IS) IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS IS CONSTITUTES CONSENT TO MONITORING.

Figure 9.2. (U) Warning Label.

9.3.3 (U) Action to be Taken Before Monitoring

Do not proceed to monitor an individual (targeted monitoring) without first gaining permission and guidance from General Counsel and Commander/CO/SIO. Unauthorized targeted monitoring is a

violation of the subject's rights and may jeopardize the investigation. Authorization for targeted monitoring must come through the Commander/Commanding Officer in consultation with legal representation by the Judge Advocate General (JAG), General Counsel, or an authorized investigative organization, such as the (Defense Criminal Investigative Service (DCIS), US Army Criminal Intelligence Department (USACID), US Army Military Intelligence (USAMI), Naval Criminal Investigative Service (NCIS), or Air Force Office of Special Investigations (AFOSI)). The ISSM and ISSO/SA will make every effort to take action in Table 9.1 and answer all applicable questions identified in Table 9.2.

9.3.4 (U) Review System Specific Security Features

The investigators will want full documentation on many aspects of the system being violated. Table 9.2 identifies sample information needed by the Commander/CO/SIO that may be needed in justifying the investigation. The ISSM and ISSO/SA will make every effort to document the information in Table 9.2.

Table 9.1. (U) Recommended Incident Response Actions

ITEM NUMBER	ACTION RECOMMENDED
1	Notify the ISSM.
2	The ISSM will notify the Special Security Officer (SSO), Commander/CO/SIO
3	The Commander/CO/SIO will coordinate with the General Counsel and authorized investigative office for formal guidance.
4	Follow Chapter 8 for incident reporting
5	Keep a record of actions by the ISSM concerning the incident.

Table 9.2. (U) Sample Monitoring Investigation Questions

ITEM NUMBER	SAMPLE INFORMATION THAT MAY BE NEEDED BY THE COMMANDER
1	What event(s) triggered suspicion of improper system use?

2	Does the system have a warning banner? Is the banner displayed prior to the first keystroke?
3	Where is the hardware physically located?
4	What level of classified data is processed on the system?
5	What organization/activity is supported by the system?
6	What connectivities are authorized to the system?
7	What is the function of the system?
8	What security software, if any, is used on the system?
9	Are audit trails running normally and have they been reviewed regularly?
10	Is a copy of the SSAA/SSP available?

CHAPTER 10 - MALICIOUS CODE PREVENTION

10.1 (U) PURPOSE

Minimize the risk of malicious code (malicious logic) from being imported to or exported from Information Systems (ISs). Preventing malicious code is everyone's responsibility. This chapter identifies various types of malicious code and provides preventive measures to avoid problems.

10.2 (U) SCOPE

The provisions of this policy apply to all organizations processing SCI, their components, and affiliates worldwide, as well as all contractor-owned or operated systems employed in support of SCI designated contracts. This supplement will be specified on all DD Forms 254 as a contractual requirement. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

10.3 (U) DEFINITIONS

10.3.1 (U) Malicious code

Malicious code is that which is intentionally included in hardware, software, firmware or data for unauthorized purposes. Computer Viruses, Worms, Trojan Horses, Trapdoors, and Logic/Time Bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to ISs because of their reproductive capability. Malicious code can arrive through either media that are introduced to ISs or as mobile code that arrives through connections to other systems and networks.

10.3.2 (U) Mobile Code

Mobile code is technology that allows for the creation of executable information which can be delivered to an information system and then directly executed on any hardware/software architecture that has an appropriate host execution environment. The code can perform positive or negative actions (malicious). The focus on risk is based on the receipt of executable information from sources outside a Designated Approval Authority's area of responsibility or control. Mobile code is the software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

Refer to the Intelligence Community Chief Information Officer (ICCIO) Intelligence Community Policy for the Use of Mobile Code in the Intelligence Community System for Information Sharing (ICSIS) Environment, dated 08 August 2002 for additional guidance.

10.3.3 (U) Malicious Mobile Code

Mobile code is the software designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access

to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources. Types of mobile code are direct and indirect.

- Direct mobile code can be recognized within the primary transport mechanism, such as a virus within a file.
- Indirect mobile code may be embedded, such as inside of an attachment to E-Mail.

10.3.4 (U) Mobile Code Technologies

Software technologies that provide the mechanisms for the production and use of mobile code are grouped into three Risk Categories based on the functions performed by the code, the ability to control distribution of the code and control of the code during execution.

Mobile Code is categorized based on the assessed risk posed to the IC:

- Red Mobile Code has been assessed as a high risk and shall be prohibited from use unless a specific exception is granted by the IAPB.
- Yellow Mobile Code has been assessed as a medium risk and shall only be used on a case-by-case basis after implementing explicit IC-approved mitigations as specified in the Applications, Services and Protocols Categorization List (ASPCL).
- Green Mobile Code has been assessed as a low risk and shall be permitted for use throughout the IC.

10.3.4.1 (U) Red Mobile Code

Red Mobile Code can exhibit broad functionality using unmediated access to services and resources of workstations, hosts and remote systems. Red Mobile Code technologies can pose severe threats to IC services. Some of these technologies allow differentiation between unsigned and signed code (i.e., a mechanism used by a trusted source), with capabilities to configure systems so that only signed code will execute. Examples of Red Mobile Code technologies can be found on the ICCIO ASPCL Mobile Code Technologies web page listed below.

10.3.4.2 (U) Yellow Mobile Code

Yellow Mobile Code has full functionality using mediated or controlled access to services and resources of workstations, hosts and remote systems. Yellow Mobile Code technologies may employ known and documented fine-grain, periodic, or continuous countermeasures or safeguards against malicious use. Some of these technologies allow differentiation between unsigned and signed code (i.e., a mechanism used by a trusted source), with capabilities to configure systems so that only signed code will execute.

Yellow Mobile Code technologies can pose a medium threat to IC information systems. The use of Yellow Mobile Code technologies, when combined with prudent countermeasures against malicious use, can afford benefits that outweigh their risks. Yellow Mobile Code may be used through CIs, and shall only be used with the IC-approved mitigations and countermeasures specified in the Applications, Services, and Protocols Categorization List (ASPCL) located at (http://www.iccio.ic.gov/docs/side_menu/security/CASPER/ASPCL_Mobile_Code_Technologies.asp.) Additional mitigations or countermeasures may be applied at the discretion of the DAA. Examples of Yellow Mobile Code technologies can be found on the ICCIO ASPCL Mobile Code Technologies web page.

10.3.4.3 (U) Green Mobile Code

Green Mobile Code has limited functionality, with no capability for unmediated or uncontrolled access to services and resources of workstations, hosts and remote systems. Green Mobile Code technologies may employ known and documented fine-grain, periodic, or continuous countermeasures or safeguards against malicious use. Protection against these types of mobile code only requires normal vigilance compared with that required to keep any software configured to resist known exploits. Green Mobile Code shall be allowed through Controlled Interfaces (CI) without restriction. Examples of Green Mobile Code technologies can be found on the ICCIO ASPCL Mobile Code Technologies web page listed above.

10.3.4.4 (U) Emerging Mobile Code Technologies

Emerging technologies refer to any Mobile Code technologies or languages whose capabilities and threat level have not yet been categorized. Emerging technologies pose uncertain risk to the IC systems.

Therefore, Any Mobile Code that has not been assessed or validated (i.e., it is not listed in the ASPCL) shall be automatically considered Red

10.3.4.5 (U) Exempt technologies

Those that are not considered true mobile code. These include:

- XML;
- SMIL;
- QuickTime;
- VRML (exclusive of any associated Java Applets or JavaScript Scripts);
- Web server scripts, links and applets that execute on a server (Java servlets, Java Server Pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side Lotus Script);
- Local programs and command scripts that exist on a user workstation (binary executables, shell scripts, batch scripts, Windows Scripting Host (WSH), PERL scripts);
- Distributed object-oriented programming systems that do not go back to the server to execute objects (CORBA, DCOM); and
- Software patches, updates and self-extracting updates that must be explicitly invoked by a user (Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins, and Linux Update Manager)

10.3.5 (U) Trusted Source

A trusted source is a source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication. The following mechanisms are sufficient to validate the identity of a trusted source:

- a connection via JWICS;
- a connection via the SIPRNET;
- a digital signature over the mobile code itself using either DoD or IC-approved PKI certificate;
- a commercial certificate approved by either the DoD CIO or the IC CIO; or

- authentication of the source of the transfer by public key certificate (e.g., S/MIME, SSL server certificate from an SSL web server).

10.3.6 (U) Screening

Screening is a preventive measure to monitor processes and data to intercept malicious code before it is introduced to an IS. Screening also includes monitoring IS for the presence of malicious code which is already present. Malicious code occurs in different forms, which may have different methods for screening.

10.4 (U) PROCEDURES

The ISSM/ISSO is responsible for ensuring that the following procedures are followed.

10.4.1 (U) Preventive Procedures

Scan all information storage media (e.g., diskettes, compact disks, computer hard drives, etc.) and E-mail attachments introduced prior to its use on any SCI system. If the media cannot be scanned then it is considered high risk and cannot be used on any SCI system without approval from the SCO. Procedures to be followed:

- Use automated scanning applications, e.g., virus scanning, which will monitor media upon introduction to a system and data being transferred into the IS.
- Check and review the IS operating environment for the presence of malicious code on a frequent basis.
- Avoid hostile mobile code through use of only authorized/verified and registered mobile code.
- Keep automated scanning processes up to date with the most current recognition signatures.
- Ensure that users will not knowingly or willfully introduce malicious code into systems.
- Ensure that users will not import or use unauthorized data, media, software, firmware, or hardware on systems.
- Ensure that users will conduct screening of all incoming data (e.g., E-Mail and attachments) if this process is not automated.
- Ensure that users will not use personal-owned media (e.g., music, video, or multimedia compact disks) in Government-owned IS.
- Ensure that all users immediately report all security incidents and potential threats and vulnerabilities involving malicious code on ISs to the ISSM.
- Controlled Interfaces with malicious code scanning capability does not relieve the management of the receiving IS from the responsibility of also checking for malicious code.

10.4.2 (U) Malicious Code Detection

If a malicious code is detected or a presence of malicious code is suspected on any IS, do the following:

- Immediately report it to the ISSM for further instruction IAW Chapter 8. Do nothing that might cause the further spread of the malicious code.
- Take the following corrective actions:
- If found in a file, use approved Anti-virus software to remove a virus from a file.

- If found on a System, use approved Antivirus software to remove the virus from your system.
- If files are corrupted, then restore affected files from system backups.

10.5 (U) MALICIOUS CODE SECURITY REQUIREMENTS

An integral part of this program is the mandatory training required by public law. Users shall receive initial training on prescribed IS security restrictions and safeguards prior to accessing corporate IS assets IAW Chapter 6. User awareness is still the first line of defense, especially since there is NO ANTI-VIRUS SOFTWARE THAT CAN GUARANTEE 100% PROTECTION FROM VIRUSES.

10.5.1 (U) Preventative Steps to be Taken

- Employ user awareness education.
- Use virus scanning programs to detect viruses that have been placed on diskettes.
- Never start a PC while a diskette is in the drive.
- Ensure the CMOS boot-up sequence for PCs is configured to boot-up from the hard drive first (usually the C: drive) NOT the A: drive.
- Block receiving/sending of executable code. Blocking files with executable extensions such as EXE, VBS, SHS etc., contributes to overall anti-virus measures.
- Adopt procedures to configure email applications to view received files/attachments in a “viewer.” Viewers normally do not have macro capabilities.
- Do not use a diskette from an outside source without first scanning it for potential viruses.
- Do not download data from Internet bulletin boards, etc.
- Ensure files are being backed up daily.
- Implement a process to routinely check security bulletins for updates, (i.e., CERT, AFCERT, NAVCERT, etc.)
- Whenever possible, disable the automatic execution of all categories of mobile code in email bodies and attachments.
- Whenever possible, desktop software shall be configured to prompt the user prior to opening email attachments that may contain mobile code.

CHAPTER 11 - SOFTWARE

11.1 (U) PURPOSE

This chapter defines the various types of software applications that may be used on any DoD IS. It lists software types that are authorized as well as specific types of software that are not authorized.

11.2 (U) DEFINITION

For the purpose of this policy, software should be interpreted to be any information recorded on any information storage media to include data files, source code and executable code.

11.3 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

11.4 (U) PROCEDURES FOR SOFTWARE AUTHORIZATION

Additions or modifications to software on systems which affects system accreditation must be evaluated by the ISSM through the local CMB/CCB process and coordinated with the DAA Rep/SCO to gain concurrence.

11.5 (U) LOW RISK SOFTWARE

Low risk software must be approved by the ISSPM/ISSM before introduction to SCI ISs, including the following guidelines:

- Provided officially by another U.S. Government Agency that has equivalent standards.
- Provided under contract to organizations involved with the processing of SCI and related intelligence information.
- Developed within a Government-approved facility.
- COTS software provided through appropriate procurement channels.
- Distributed through official channels.
- Acquired from a reputable vendor for official use or evaluation (i.e., maintenance diagnostic software).

NOTE: In all cases, system and site specific security policy should be considered.

11.6 (U) HIGH RISK SOFTWARE

Certain software is deemed “high risk” and is not authorized for use without approval. The respective DAA Rep/SCO must approve such software in writing before it may be legally used. High risk software includes public domain, demonstration software, and embedded software not obtained through official channels. The DAA Rep/SCO may deem other software high risk.

11.6.1 (U) Public Domain Software

Only the DAA (Rep)/SCO may approve the use of public-domain software. Do not confuse public-domain software with off-the-shelf, or user developed software. A request to use public-domain software and the subsequent approval requires an extensive evaluation, by approved evaluation centers, of the particular software source code in search of Trojan Horses, Trapdoors, Viruses, etc. There is limited capability to perform these required evaluations.

11.6.2 (U) Demonstration Software and Media

Floppy diskettes and removable hard disks used for demonstrations, with the intent of being returned to a vendor, must be processed on a computer that has never processed or stored classified data. Otherwise, the demonstration media cannot be released back to the vendor and should be destroyed. If it is to be returned to the vendor, a fully cleared and indoctrinated individual must verify that the media was used only in an unclassified computer.

NOTE: Vendor hardware used for software demonstrations must operate in a stand-alone mode. If use of vendor software for demonstration purposes requires connection to a DoD network approval must be granted by the appropriate DAA Rep/SCO.

11.6.3 (U) Embedded Software

Game software included as part of a vendor bundled software or software/hardware package shall be removed from the IS immediately following the installation and testing of the software. Vendor supplied games occupy valuable disk space and could open the door for Fraud, Waste, and Abuse (FW&A) charges. Game software provided for use as tutorials may be granted as an exception to this restriction by the DAA Rep/SCO. All other games software currently on SCI ISs are considered a violation of this policy and must be removed.

11.6.4 (U) Unauthorized Software

Types of software that are not authorized include:

- Games.
- Public domain software or “shareware” which have been obtained from unofficial channels.
- All software applications which have been developed outside Government approved facilities, such as those developed on personally owned computers at home or software acquired via non- U.S. Government “bulletin boards”.
- Personally owned software (either purchased or gratuitously acquired).
- Software purchased using employee funds (from an activity such as a coffee fund).
- Software from unknown sources.
- Illegally copied software in violation of copyright rules.
- Music and video or multimedia compact disks not procured through official Government channels.

11.6.5 (U) IA Software and Security Tools

When employing evaluated and validated IA/IA enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. Some high risk software may be required to meet system requirements. For example, to comply with paragraph 4.B.2.a.5.b of DCID 6/3, intrusion/attack detection and monitoring tools are required to support required periodic testing by the ISSO/ISSM within their domain.

CHAPTER 12 - INFORMATION STORAGE MEDIA

12.1 (U) PURPOSE

This chapter outlines the minimum requirements for the control and accounting of information storage media. The Commander/Commanding Officer is responsible to prescribe the policy for the level of control and accounting appropriate for information storage media under his/her control. Also, this chapter outlines the minimum requirements for marking the magnetic media and paper products. Labeling of magnetic media is similar to labeling paper products. Like paper documents, all information storage media must be properly marked with the appropriate classification and handling instructions.

12.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

12.3 (U) CONTROL AND ACCOUNTING PROCEDURES

This chapter provides guidelines for control and accounting of information storage media. For any system that operates with PL-3 or lower functionality, media that is not write-protected and is placed into that system must be classified at the highest level of information on the system until reviewed and validated. Media accountability will be based on the determined classification level of the media.

12.3.1 (U) Information Storage Media Control

Per DoD 5105.21-M-1, there is a requirement to control and account for certain information storage media within functional categories. This chapter tasks the organization Commander/Commanding Officer with developing a unit-unique SOP for control and accountability.

12.3.1.1 (U) Inspections

The organization must be able to demonstrate positive control and accounting of information storage media according to its SOP when being inspected by authorities.

12.3.1.2 (U) Control Procedures

Control of information storage media should begin upon introduction into the organization according to DoD 5105.21-M-1, and local SOP.

12.3.1.3 (U) Other Categories of Storage Media

The following major categories of information storage media should be considered for accountability in compliance with copyright and licensing as documented in the SOP:

- COTS and vendor software.

- Government developed software.
- Other organization unique software and data.

12.3.2 (U) Audits and Reports

Each organization will periodically audit the information storage media accountability records for accuracy. The frequency of audits should depend on the volume of media on hand, the frequency of changes in the accounting system, criticality of the media, and classification level of data stored onto the media. Perform other audits at the Commander's/Commanding Officer's discretion. Document the result of these audits in an internal report to remain on file within the organization for at least one year. Report discrepancies to the ISSM for further reporting to the DAA Rep/SCO as required. These requirements should be addressed in the organization SOP along with the following:

- (U) Inventories/audits will be required for accountable information storage media per DoD 5105.21-M-1.
- (U) Information storage media holdings will be audited periodically to ensure proper control is being maintained and media is destroyed when no longer needed.

12.3.3 (U) Destruction of Media

See Chapter 21, for guidance on the proper destruction of media.

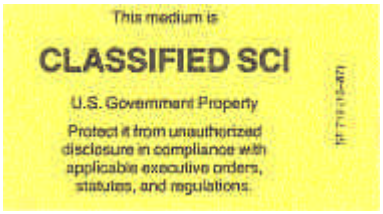
12.4 (U) MEDIA LABELING PROCEDURES

To ensure data integrity and protection, information storage media must be administratively labeled and appropriately protected to prevent the loss of information through poor security procedures. Likewise, to prevent security compromises, all output products must be appropriately protected. Proper classification marking of output paper products, microfiche, terminal screen displays and central processing units (CPUs) must be accomplished and is the responsibility of the user. Each supervisor is ultimately responsible for the labeling, handling, and storage of both media and paper products within their assigned area of responsibility.

12.4.1 (U) Information Storage Media

Removable IS storage media and devices shall have external labels clearly indicating the classification of the information and applicable associated markings (e.g., digraphs, trigraphs). Labeling exemption for OPSEC requirements may be granted within local policy with DAA/DAA Rep/SCO concurrence. Examples include magnetic tape reels, cartridges, cassettes; removable discs, disc cartridges, disc packs, diskettes, magnetic cards and electro-optical (e.g., CD) media. All removable information storage media and devices will be marked with the appropriate Standard Form (SF) 700-series classification and descriptor labels as listed and depicted below:

- SF 706, Top Secret Label
- SF 707, Secret Label
- SF 708, Confidential Label
- SF 710, Unclassified Label
- SF 711, Data Descriptor (On all magnetic media)
- SF 712, Classified SCI Label (All classification levels)



SF 712, SCI (Yellow**)**
Includes ALL classification levels of SCI

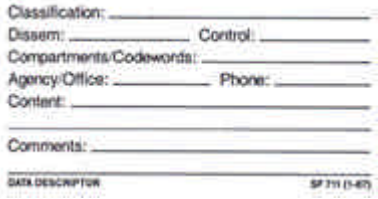
SF 706, TOP SECRET (Orange**)**

SF 707, SECRET (Red**)**

SF 708, CONFIDENTIAL (Blue**)**

SF 709, GENERIC CLASSIFIED (Purple**)**
For use on removable media ONLY

SF 710, UNCLASSIFIED (Green**)**
Unclassified Information ONLY



SF 711, Data Descriptor Label

Figure 12.1 – SF 700 Series Labels

12.4.1.1 (U) Label Placement

See the Federal Register 2003 and applicable military department regulations for exact placement procedures. Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media. Labels for Compact Disks (CDs) must NOT be placed on the CD itself. Place the labels on the CD container or envelope. Record the classification and accounting number in the "Control" block of the SF 711 and write the same number on the CD with a Paint-pen, CD label maker or permanent marker. The number should not interfere with the operation of the CD. Notice: Do not use pens that contain toluene.

12.4.1.2 (U) Data Descriptor Label

The SF 711, Data Descriptor Label, identifies the content of a specific media to include unclassified, collateral-classified, and SCI. An SF 711 is not required if the disk bears the following information: Organization, office symbol, classification, and media sequence number (if locally

required). The user fills in the "Classification", "Dissem", "Control", and "Compartments/Codewords" blocks as appropriate.

12.4.2 (U) Tactical/Deployable Labeling media and hardware components

The following labeling requirements should have OPSEC considerations prior to implementing.

- Security requirement: Removable media and IS hardware components should be labeled IAW Chapter 12.
- Operational requirement: OPSEC requirement to disguise the existence of classified information on an IS (including specification of compartments).
- Sample security implementation: Reusable deployed hardware sanitized for travel (media removed) is shipped via commercial carrier to its intended destination, no labels present.

12.4.3 (U) Classification Markings

All documents residing or processed on information storage media/ISs will be marked IAW the Controlled Access Program Coordination Office (CAPCO) guidance "Intelligence Community Classification and Control Markings Implementation Manual", dated 10 Sep 1999 (Amended 21 March 2002), DoD 5105.21-M-1, dated August 1998, or appropriate Agency/Service regulations.

The guidance references are located at:

http://www.cms.ic.gov/Capco/Pages/Markings%20Implementation%20Manual/TOC.htm

http://www.dia.ic.gov/admin/ds/sy/sys/sys-4/regs_mans_and_procs/infosec_regman.html

CHAPTER 13 - INFORMATION SYSTEMS (IS) MAINTENANCE PROCEDURES

13.1 (U) PURPOSE

The purpose of this chapter is to identify security procedures and responsibilities that must be followed during the maintenance of ISs. ISs are particularly vulnerable to security threats during maintenance activities. The level of risk is directly associated with the maintenance person's clearance status (cleared or uncleared). A maintenance person may be uncleared or may not be cleared to the level of classified information contained on the IS. Properly cleared personnel working in the area must maintain a high level of security awareness at all times during IS maintenance activities. Additionally, the ISSM is responsible for IS maintenance security policy, including maintenance procedures for all ISs under his or her control.

13.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

13.3 (U) PROCEDURES

13.3.1 (U) Maintenance Personnel

13.3.1.1 (U) Maintenance by Cleared Personnel

Personnel who perform maintenance on classified systems should be cleared and indoctrinated to the highest classification level of information processed on the system. Appropriately cleared personnel who perform maintenance or diagnostics on ISs do not require an escort. However, an appropriately cleared and, when possible, technically-knowledgeable employee should be present when maintenance is being performed to assure that the proper security procedures are being followed.

13.3.1.2 (U) Maintenance by Uncleared (or Lower-Cleared) Personnel

If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used provided a fully cleared and technically qualified escort monitors and records their activities in a maintenance log.

- Uncleared maintenance personnel should be US citizens. Outside the US, where US citizens are not available to perform maintenance, foreign nationals may be utilized, but only with DAA Rep/ SCO approval.
- Prior to maintenance by uncleared personnel, the IS will be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, ISSM-approved procedures will be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive data that is contained on the system.
- A separate, unclassified copy of the operating system (e.g., a specific copy other than the copy(s) used in processing information), including any floppy disks or cassettes that are integral to the

operating system, will be used for all maintenance operations performed by uncleared personnel. The copy will be labeled "UNCLASSIFIED—FOR MAINTENANCE ONLY" and protected IAW procedures established in the SSAA/SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident will be considered and approved by the ISSM on a case-by-case basis.

13.3.2 (U) General Maintenance Requirements

13.3.2.1 (U) Maintenance Log

A maintenance log must be maintained for the life of the IS. The maintenance log should include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts. Maintain this log for the life of the IS.

13.3.2.2 (U) Location of Maintenance

Maintenance should be performed on-site whenever possible. Equipment repaired off-site and intended for reintroduction into a SCIF may require protection from association with that particular SCIF or program.

13.3.2.3 (U) Removal of Systems/Components

If systems or system components must be removed from the SCIF for repair, they must first be purged, and downgraded to the appropriate classification level, or sanitized of all classified data and declassified IAW ISSM-approved procedures. The ISSM, or designee, must approve the release of all systems and parts removed from the system, in accordance with Chapter 20.

13.3.2.4 (U) Use of Network Analyzers

Introduction of network analyzers that provide maintenance personnel with a capability to do keystroke monitoring must be approved by the ISSM, or designee, prior to being introduced into an IS.

13.3.2.5 (U) Use of Diagnostics

If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a SCIF, the media containing the programs must be checked for malicious codes before the media is connected to the system, must remain within the SCIF, and must be stored and controlled at the classification level of the IS. Prior to entering the SCIF, maintenance personnel must be advised that they will not be allowed to remove media from the SCIF. If deviation from this procedure is required under special circumstances, then each time the diagnostic test media is introduced into a SCIF it must undergo stringent integrity checks (e.g., virus scanning, checksum, etc.) prior to being used on the IS and, before leaving the facility, the media must be checked to assure that no classified information has been written on it. Such a deviation must be approved by the ISSM.

13.3.2.6 (U) Introduction of Maintenance Equipment into a SCIF

All diagnostic equipment or other items/devices carried into a SCIF by maintenance personnel will be handled as follows:

- Systems and system components being brought into the SCIF shall, as far as practical, be inspected for improper modification.

- Maintenance equipment that has the capability of retaining information must be appropriately sanitized by established procedures (see Chapter 21) before being released. If the equipment cannot be sanitized, it must remain within the facility, be destroyed, or be released under procedures approved by the DAA Rep/SCO.
- Replacement equipment or components that are brought into the SCIF for the purpose of swapping-out facility components are allowed. However, any component introduced into an IS will remain in the facility until proper release procedures are completed.
- Devices with transmit capability (e.g., IR, RF, etc.) shall remain outside the SCIF.

13.3.3 (U) Maintenance and System Security

After maintenance, and before return to operation, the ISSM, or designee, shall check the security features on the IS to assure that they still function properly. Additionally, any maintenance changes that impact the security of the system shall receive a configuration management review.

13.3.4 (U) Remote Maintenance Requirements/Considerations

- The Installation and use of remote diagnostic links must be preapproved and procedures addressed in the SSAA/SSP.
- An audit log shall be maintained for five years of all remote maintenance, diagnostic, and service transactions and periodically reviewed by the ISSO/ SA.
- Other techniques to consider when remote maintenance is required include encryption and decryption of diagnostic communications, strong identification and authentication techniques such as tokens and remote disconnect verification.

13.3.4.1 (U) Maintenance Performed with the same Level of Security

Remote Diagnostic Maintenance service may be provided by a service or organization that does possess the same level and category(ies) of security. The communications links connecting the components of the systems, plus associated data communications and networks, shall be protected IAW national security policies and procedures applicable to the sensitivity level of the data being transmitted.

13.3.4.2 (U) Maintenance Performed with a different Level of Security

If remote diagnostic or maintenance services are required from a service or organization that does not provide the same level of security required for the IS being maintained, the system must be cleared; placed in a standalone configuration prior to the connection of the remote access line; and maintenance personnel must possess the appropriate clearance to perform the maintenance. If the system cannot be cleared (e.g., due to a system crash), remote diagnostics and maintenance shall not be allowed.

13.3.4.3 (U) Initiating and Terminating Remote Access

The initiation and termination of the remote access must be performed by the ISSM or designee.

13.3.4.4 (U) Keystroke Monitoring Requirements

Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. So far as practicable, a technically qualified person shall review the maintenance log to assure the detection of unauthorized changes. The ISSM, or designee, will assure that maintenance technicians

responsible for performing remote diagnosis/maintenance are advised (contractually, verbally, banner, etc.) prior to remote diagnostics/maintenance that keystroke monitoring will be performed.

13.3.5 (U) Life Cycle Maintenance

The requirement for, and vulnerabilities of, IS maintenance, whether performed by military or contractor personnel, must be addressed during all phases of the system's life cycle. The security implications of IS maintenance must be specifically addressed when entering into contract negotiations for any maintenance activity.

CHAPTER 14 – DIGITAL AND MULTI-FUNCTION DEVICES (COPY/PRINT/SCAN/FAX)

14.1 (U) PURPOSE

This section provides the guidance for the acquisition and life-cycle maintenance for multi-function devices having the capability to copy, print, scan, and fax, either in a standalone mode or networked. These devices include digital copiers, copier or printer centers. These devices are computer driven and therefore constitute as an Information System (IS) and are subject to many of the same security vulnerabilities as any other computer devices.

These computer-based, network-capable devices with processors, memory, hard-drives, image retention components, and, in some cases, cellular phone transmitters with vendor auto-alert features, are to be classified as IS equipment and are governed by organizational information systems security policies. Some concerns are memory capability, service technician laptop connectivity, repair capabilities and remote diagnostics.

Job queues are capable of holding up to 1500 images or more, depending on the size and complexity of the images. These images are compressed and encrypted with built-in proprietary capabilities. Under normal circumstances these images are not accessible but may be copied and later opened by technically competent personnel. All images retained in the memory remain in the memory until over-written by subsequent printing images. The memory is non-volatile, so if power is lost the images remain on the hard drive. This creates a problem when service technicians respond to repair the unit. The laptop computer utilized by the service technicians has the capability of downloading the information stored in the copy/printer center's hard drive. Although this information may be compressed and encrypted with proprietary encryption capabilities, technically competent personnel may later retrieve the information.

14.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

14.3 (U) POLICY

These multi-function printer/copier devices have to meet the same Certification and Accreditation (C&A) requirements as specified in references and internal C&A process requirements. They are under the management of the organizations' Designated Accrediting Authority. Additionally:

- In the event that any key provisions regarding these multi-function printer/copier devices cannot be met, associated risks must be identified and a waiver request submitted for approval to the DAA or their representative, who has the sole authority to grant exceptions to this policy.
- Networked multi-functional printer/copier devices are only permitted to process information at the accredited classification level of the network itself.
- When connected to a network, multi-functional printer/copier devices will assume the highest classification for which the network is accredited and, if also operated as a standalone device, they

will assume the highest classification of copied documents. It should be kept in mind when using multi-functional printer/copier equipment that the document image will remain on the imaging drum/belt, hard drives, and static RAM.

14.4 (U) PROCEDURES

Since these copiers have internal electronic memory components it is necessary to purchase them outright (not lease them) and maintain absolute control of all electronic parts that contain a memory/data remanence capacity, and to have a maintenance contract that provides for maintenance support by cleared personnel. The only exceptions to this maintenance policy are specified in Section 8.B.8.b. of DCID 6/3.

- If laptops are required for diagnostics, they must be purchased (software included) and maintained in appropriate secure facilities. The service technician must not be permitted to connect a proprietary laptop to the copy/printer center as the technician may download classified information onto the laptop. Nor may the copy/printer center, primarily the hard drive, be removed from the SCIF to a non-SCIF area. Consideration should be given to obtain a proper security clearance for the service technician and provide a government laptop with proprietary diagnostic and repair information installed. The laptop must remain within the classified area and may not be utilized by personnel other than the repair technician.
- Purchase the copy/printer center with a removable hard drive vice an internal hard drive. Consideration for a second hard drive for diagnostic and repair only should be available to allow the service technician lap top connectivity. The built-in internal hard drive may be extremely difficult to access and remove, requiring disassembly. The classified information stored on the hard drive is the property of the United States and must not be released outside official channels.
- Whether previous systems have been purchased or leased with either an internal or removable hard drive, you are required to purchase a second replacement hard drive. Usually under lease agreements, the equipment must be returned with all parts. Once the hard drive is removed, it can then be replaced with the second non-classified hard drive for turn-in and the lease agreement should then remain valid.
- Removal/return of purely mechanical or electro-mechanical parts to a vendor will only be permitted based on a risk determination that includes consideration of threat, vulnerability, impact, and cost. Printed circuit boards/memory boards are to be destroyed as classified trash. It is advised that no parts should be released in overseas locales, or other high counterintelligence threat areas. The cognizant Security Officer, Special Security Officer (SSO), Information Systems Security Officer (ISSO), or Contractor Security Officer (CSO), is responsible for on-site decisions. The only exception permitted is if a part can be absolutely cleansed in accordance with the documented guidance in Chapter 20 of this document.
- All communications ports not specifically required for networked or contractual maintenance must be removed or permanently disabled. Only hardwired connections are permitted (no IR, RF, or Audio communications). This provision must be included in the purchase contract.
- Passwords are set at the factory. Some of these passwords can be changed by the user, however some passwords can not. Additionally, all factory set passwords are the same for each machine. Ensure the passwords have been changed by the ISSO/ISSM where feasible.
- The site SSO shall make information regarding installation of new copiers and major repairs to existing copiers available to Technical Security evaluators.

- The Equipment Receiving Facility shall physically inspect incoming shipments for evidence of tampering.

14.4.1 (U) FAX Capabilities

The multi-function printer/copier devices may contain a cellular telephone with FAX capability. The FAX is usually factory set to automatically send a page (i.e., once every 100 copies) to the manufacturer so the manufacturer can ensure quality copies. A firewall should be installed between the FAX and the hard drive or have the FAX capability disabled.

14.5 (U) RESPONSIBILITIES

14.5.1 (U) The DAA representative shall:

- Ensure that system owners provide appropriate Certification and Accreditation documentation/authorizations to the DAA
- Inform their customers of this policy.

14.5.2 (U) ISSOs and/or Information Systems Security Managers shall:

- Ensure that each user receives appropriate awareness training;
- Ensure that installed systems meet the TEMPEST standards of NSTISSP 300, “National Policy on Control of Compromising Emanations”;
- Ensure that appropriate classification and usage labels are properly affixed to the equipment;
- Update all SSPs/SSAAs to reflect copier locations, model and serial numbers. In addition to the SSP/SSAA, the Certification and Accreditation package should include maintenance procedures which comply with the policies specified in this document; and
- Ensure the management of packaging, shipping, receiving, and inspection processes by trusted vendors. For added security, the application of tamper evident seals is recommended.

14.5.3 (U) USERS shall:

- Notify their ISSO, ISSM, or ISSPM in advance of the purchase of Multi-functional printer/copier devices to ensure SSPs/SSAAs are created or updated as appropriate, and approved prior to purchase;
- Protect the peripherals (copiers) located in their area in accordance with local/organizational policies;
- Safeguard the output in accord with daily security checklist procedures if there is no name on an output that can be attributed to an individual;
- Report any IS security incidents in accord with local/organizational procedures; and
- Adhere to their responsibilities as an IS User and as outlined in local/organizational policies and procedures.

CHAPTER 15 - PORTABLE ELECTRONIC DEVICES

15.1 (U) PURPOSE

This chapter identifies procedures for the entry and exit of portable electronic devices into SCIFs. A portable electronic device is a generic term used to describe the myriad of small electronic items that are widely available. The rapid growth in technological capabilities of portable electronic devices/portable computing devices (PEDs/PCDs) has led to concerns about their portability into and out of SCIFs. PEDs include cellular telephones, two way pagers, palm sized computing devices, two-way radios, audio/video/data recording, playback features, personal digital assistants, palm tops, laptops, notebooks, data diaries, and watches with communications software and synchronization hardware, that may be used to telecommunicate. These devices must be closely monitored to ensure effective control and protection of all information on our IS.

15.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

15.3 (U) RISK

Because PEDs are designed to freely and openly exchange information, most users may not be aware of the technologies that reside in the various PEDs. PEDs may contain wireless or infrared capabilities. Thus, users do not always know when automated information transfer is active or that the PED is being reprogrammed or reconfigured remotely without their knowledge

15.3.1 (U) Classified Information

The introduction of unauthorized classified information to a PED, will result in a security violation (see Chapter 8). For example: aggregation of data, inadvertent wireless connection, and POCs maintained through classified or sensitive contracting mechanisms. If this occurs to an unclassified PED, the PED needs to be controlled as classified material (e.g., this could include confiscation of the PED). If a PED is already classified, and unauthorized classified information is found (higher than authorized for the PED), the PED needs to be controlled at the higher, more restrictive level.

15.4 (U) PROCEDURES

The use of PEDs in a SCI environment presents a high degree of risk for the compromise of classified or sensitive information. PEDs will only be used to fulfill mission requirements. Additionally, very specific handling procedures must be developed and made available to the user of the PED. The Agency in charge of any given SCIF is the authority for the procedures to move PEDs in or out of their facilities.

15.4.1 (U) Approval Requirements

All of the following requirements must be satisfied prior to approving the use of portable electronic devices:

15.4.1.1 (U) Personal PEDs

- Personal PEDs, hardware/software associated with them, and media are prohibited from entering/exiting a SCIF unless authorized by the Agency granting SCIF accreditation.
- Personal PEDs are prohibited from operating within a SCIF unless authorized by the agency granting SCIF accreditation. If approved, the owner of these devices and his/her supervisor must sign a statement acknowledging that they understand and will adhere to the restrictions identified below.
- Connection of a Personal PED to any IS within a SCIF is prohibited.
- PEDs with wireless, Radio Frequency (RF), Infrared (IR) technology, microphones, or recording capability will not be used unless these capabilities are turned off or physically disabled (i.e., metallic tape over IR port(s)).

15.4.1.2 (U) Government Owned PEDs

- Government PEDs, hardware/software associated with them, and media must be controlled when entering/exiting a SCIF.
- Government PEDs are prohibited from operating within a SCIF unless authorized and accredited by the agency granting the SCIF accreditation. As part of the accreditation requirements, the user of these devices and his/her supervisor must sign a statement acknowledging that they understand and will adhere to the restrictions identified below.
- Connection of a Government PED to any IS within a SCIF must be approved by the ISSM in writing.
- PEDs with wireless, RF, IR technology, microphones, or recording capability will not be used unless these capabilities are turned off or physically disabled (i.e., metallic tape over IR port(s)).
- Specified PEDs may be used to process classified information. In addition, these PEDs may be granted approval to connect to ISs on a case-by-case basis in writing by the ISSM. Specified PEDs approved to process classified information must meet minimum technical security requirements will be determined by the ISSM.
- If approved, the PED and associated media must be transported and stored in a manner that affords security sufficient to preclude compromise of information, sabotage, theft, or tampering. Procedures for handling the PED in a SCIF must be available and provided to the user.

15.4.1.3 (U) Contractor Business Owned PEDs

- Contractor Business Owned PEDs will follow all requirements identified in paragraph 15.4.1.2.
- All Contractor Business Owned PEDs must support a specific Government contract. Documented identification of the equipment in support of the contract must be provided prior to entry into a SCIF.

15.4.2 (U) Handling Procedures

When it has been determined that the use of PEDs is absolutely necessary to fulfill mission requirements, and the requirements set forth in paragraph 15.4.1 are satisfied, the following procedures must be implemented and followed.

15.4.2.1 (U) Standard Operating Procedure (SOP) Development

The responsible organization must develop a case specific SOP and/or ensure procedures are addressed in the site CONOPs. The following information must be considered and, where applicable, included in the SOP:

- The SOP must include the organization and name of the ISSM and SSO responsible for the issue and control of PEDs.
- Prior to the introduction of PEDs into a SCIF, it must be approved by the appropriate security personnel having security cognizance for the facility.
- PEDs must operate within one common accredited security parameter (i.e., protection level/level of concern, classification, etc.) as approved by the DAA Rep/SCO.
- All programs, equipment or data diskettes used with the PED must be marked with a label identifying the appropriate classification. Labeling exemption for OPSEC requirements may be granted within local policy with DAA/DAA Rep concurrence.
- If unauthorized classified information is identified on a PED, procedures for control of the information and the PED must be established. For example, classified information on an unclassified PED may result in confiscation of the device as an incident (see Chapter 8).
- Every effort should be made to ensure that security control features are implemented when possible (e.g., access control through userid/password).

15.4.2.2 (U) SOP Approval

The organization requesting the use of PEDs must submit the SOP (as part of the certification and accreditation documentation) to the ISSM/SSO for coordination and approval.

CHAPTER 16 - SECURITY PROCEDURES FOR INFORMATION SYSTEMS (IS) AND FACSIMILE (FAX) USE OF THE PUBLIC TELEPHONE NETWORK

16.1 (U) PURPOSE

This chapter outlines the minimum-security requirements for the control and accounting of ISs and facsimile (FAX) use of the public telephone network. ISSM is responsible for enforcing policy for the level of control and accounting appropriate for facsimile machine(s) within his/her site. This policy should be coordinated with the SCO and the appropriate SSO. The potential for covert or inadvertent release of SBU and classified information to an unintended destination is considered to be highly probable and is reduced significantly through rigorously enforcing policies and continuously monitoring these policies.

16.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

16.3 (U) PROCEDURES

External connectivity through the use of telephones or networks requires that users take every security precaution possible to prevent the loss of National Security Information (NSI) and SBU information via the public communications systems. **Classified information shall not be transmitted, processed or stored on any unclassified facsimile or an unclassified IS with either a modem or direct digital connection.** Telephone communications, voice or digital, must meet certain installation and equipment standards to ensure security. Telephone communications to external locations using computer-telephone connections must be approved before installation and activation to minimize the threat to the information.

16.3.1 (U) FAX Connectivity

16.3.1.1 (U) FAX Approval

The SSO, in coordination with the ISSM, is the approval authority for any facsimile operated within a SCIF. Specific FAX approval authority is delegated to command/site ISSMs who may approve unclassified and secure FAX machines within a SCIF. This authority is for single mode use only. ISSMs must ensure that any/all dual mode features are disabled. Dual mode (unclassified/secure) configurations are not approved for use in any facility under DIA/NSA cognizance. Transmission of information at levels above SI/TK (i.e., accountable SCI) requires applicable program manager's concurrence. Multi-function FAX/print machines with workstation/network connectivity/permanent storage/scan and text recognition capabilities are not to be approved for use of any feature other than secure facsimile transmission. Site ISSMs exercising SCI IS approval authority for these machines must ensure the following minimum security requirements are satisfied for unclassified and classified FAX connections. For non-inspectable space sites, coordinate with the organization TEMPEST officer and telephone control

officer before installing any facsimile equipment in a secure area and for requests for telephone service IAW Telephone Security Guidelines (TSG).

16.3.1.1.1 (U) Unclassified FAX.

- Unclassified FAX machines must be clearly marked for unclassified use only and consent to monitoring notification.
- Any change of equipment or location must be locally documented, to include building/room, manufacturer/model, serial number, verification of SSO authorization and point of contact information.
- Multi-function FAX/print machines with workstation/network connectivity/permanent storage/scan and text recognition capabilities must be approved. Requests for this type of equipment should be submitted to the DAA Rep/SCO via the ISSM.
- Sites should refer to local counsel on information that can be revealed in an unclassified FAX header.

16.3.1.1.2 (U) Classified FAX

- Classified FAX is normally a connection of the output of a FAX to the input port of a STU-III/STE, whose encrypted output is connected to the unclassified telephone lines. The procedures defined in this chapter are in addition to the policy and procedures addressed in NSTISSI 3013 or other appropriate SCI regulations. ISSMs are delegated approval authority for secure FAX machines operating up to the TS/SCI SI/TK level.
- Secure FAX machines must be clearly marked for the highest level of classified information processed.
- ISSMs will ensure that all operators understand the requirement to verify the level at which their STU-III/STE is connected to the recipient's STU-III/STE and verify the level at which the recipient is cleared before transmission commences.
- Information or additional compartments above the SI/TK level cannot be processed without prior approval from the appropriate data owner.
- The STU-III/STE is designed to prevent disclosure of information while it is being transmitted. Authorized users must verify the identity and clearance level of the distant party. If there is a human interface at the remote end, a challenge and reply authentication scheme will be used.
- The ISSM should approve only certified digital Faxes. The ISSM can obtain a list of certified secure digital facsimiles from the DAA/DAA Rep/SCO.

16.3.1.1.3 (U) Non-Standard Secure Fax

A non-standard secure FAX consists of a group 3 (GS3) rated standard business FAX with an approved secure protocol adapter (SPA) and an approved STU-III/STE secure data terminal (SDT). In an effort to support cost effective alternatives to the certified list of digital Faxes, non-standard secure Faxes may be purchased and used with approval from the appropriate DAA. Memory in standard business FAX machines is not designed to meet any of the stringent requirements outlined above, and therefore cannot be trusted beyond the level of TS SI/TK when connected to an approved SPA (see www.nmic.ic.gov/security/products/secfax.html on INTELINK).

16.3.1.1.4 (U) Procedures

Each facsimile requires written SOP, or identified procedures within the site CONOPs that outline the security requirements for that system. The SOP shall be approved by the ISSM and include, at minimum, the following:

- Appropriate hardware marking requirements. For example, the unclassified facsimile must be clearly marked for the transmission of unclassified information only and must have consent to monitor stickers.
- Segregation from classified systems and media.
- Point of Contact authorized to monitor operations.
- A FAX cover sheet or equivalent will accompany each FAX transmission. This cover sheet will contain:
    - The number of pages transmitted;
    - The signature of the official approving the FAX transmission;
    - The classification level of the overall information being transmitted;
    - The sender's name and telephone number; and
    - The intended recipient's name and telephone number.
- Audit logs will be used to record the transmission of any data over a FAX connected to a STU-III/STE. These logs will be maintained for one year and must include the following information:
    - User ID;
    - Date and time of FAX transmission;
    - The classification level of the information; and
    - The recipient's name, organization and telephone number.
- The ISSM will require the following minimum information to make an appropriate evaluation:
    - Building/Room Number FAX is located;
    - FAX manufacture/model number;
    - FAX Serial number;
    - Verification that the SSO has authorized the introduction of the equipment; and
    - Point of Contact's name and phone number.
- The following information should be documented and maintained with SCIF records:
    - Location and/or location changes;
    - Justification;
    - Standard operating procedures;
    - Identification of equipment (manufacturer, model, serial number, etc);
    - Verification of SSO authorization;
    - Approval level (matches the STU-III key); and
    - Point of contact information.

16.3.1.1.5 (U) FAX Accreditation

All facsimile machines within a SCIF must be accredited. All documentation and approval letters must be maintained with SCIF records.

16.3.2 (U) Computer-FAX/Modem Connectivity

A computer-FAX/modem provides a means for a computer to communicate data via telephone modem along a wired path to a distant end.

16.3.2.1 (U) Unclassified Computer-FAX/Modem Accreditation Approval

An SSAA/SSP, fully documenting the computer equipment to be used, shall be submitted to the ISSM. The SSAA/SSP will be processed via the SSO and ISSM for approval.

16.3.2.2 (U) Physical Disconnect of Unclassified Computer-FAX/Modems

The use of acoustic coupled modems is prohibited. Therefore, the physical disconnect of unclassified computer-FAX/modem equipment from the phone lines is not required.

16.3.3 (U) Computer-Modem Connectivity

16.3.3.1 (U) Unclassified Computer-Modem Connectivity

Access to Commercial Internet Service Provider (ISP)**.** "Dial-out" computer or data terminal access can only be to those unclassified systems deemed mission essential and approved in writing by the DAA Rep/SCO. Connectivity of unclassified systems to unclassified networks that are outside of SCIFs can pose a significant security risk.

16.3.3.1.1 (U) ISP Connectivity

The following procedures and guidelines pertain to those systems connected to networks which make it possible to connect to, or communicate with, any non-DoD IS.

- The system should be configured to present an unfavorable environment to any attacker, whether internal or external. The system should have only the functionality required for mission accomplishment. All other unnecessary services should be eliminated.
- The IS should use available auditing techniques to the fullest extent possible, to ensure the system is not compromised by attacks. Attacks may occur from across the network or from a legitimate system user. The SA shall monitor audit logs regularly (preferably daily) and investigate any abnormalities which may indicate a security compromise. Any attacks detected against Government systems will be classified Confidential (at a minimum) and reported IAW Chapter 8.
- SA's should monitor all available resources that provide warnings of system vulnerabilities or on-going network attacks. Examples include advisories from the military service Computer Emergency Response Teams (CERT) (i.e., Air Force (AF) AFCERT, Navy NAVCIRT [Computer Incident Response Team], Army ACERT), and Automated Systems Security Incident Support Team (ASSIST) bulletins from the Defense Information Systems Agency (DISA).

16.3.3.1.2 (U) IS to IS Connectivity

The following procedures and guidelines deal with those systems connected only to independent IS systems, either point-to-point or within a community of interest (COI).

- The system should be configured to present an unfavorable environment to any attacker, whether internal or external. The system should have only the functionality required for mission accomplishment, eliminating unnecessary services.
- The IS should use available auditing techniques to the fullest extent possible, to ensure the system is not compromised by attacks. Attacks may occur from a legitimate system user. The SA shall monitor audit logs regularly (preferably daily) and investigate any abnormalities which may indicate a security compromise. Any attacks detected against Government systems will be classified Confidential (at a minimum) and reported IAW Chapter 8.
- SA's should monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks from connected IS. Examples include advisories from the military service Computer Emergency Response Teams (CERT) (i.e., AFCERT, NAVCIRT [Computer Incident Response Team], ACERT), and ASSIST bulletins from the DISA.

16.3.3.2 (U) Classified Computer-Modem Connectivity

The only mechanism for using a modem with classified communications is by first using NSA certified encryption mechanisms. Approval for such connections must be obtained from the DAA Rep/SCO.

- Identification and Authentication. The NSA encryption mechanism is designed to prevent disclosure of information while it is being transmitted. Authorized users must verify the identity and clearance level of the distant party. Access to a host IS must not be made using auto-answer capabilities unless the host IS enforces access controls for the connection separate from the communications link controls.

16.3.3.3 (U) Classified Computer-STU-III/STE Data Port Connectivity

The following procedures and guidelines are established for using the data port of a STU-III/STE terminal and apply to all STU-III/STE users.

- STU-III Data Port Connectivity within a SCIF. Requests for STU-III/STE data port connections will be submitted to, and evaluated by the DAA Rep/SCO, on a case-by-case basis. An SSAA/SSP shall be submitted to the appropriate DAA Rep/SCO IAW Chapters 3 and 4 as applicable.
- Identification and Authentication. The STU-III/STE is designed to prevent disclosure of information while it is being transmitted. Authorized users must verify the identity and clearance level of the distant party. Access to a host IS must not be made using auto-answer capabilities unless the host IS enforces access controls for the connection separate from the communications link controls.
- Connectivity Requirements.
    - For all connections of an IS or network to a STU-III/STE, the STU-III Security Access Control system (SACS) must be employed. Exceptions may be granted by the DAA Rep/SCO.
    - The associated STU-IIIs/STEs must be keyed to the appropriate level to protect the data contained in the ISs.
    - Community of Interest. All connected ISs using the STU-III/STE data port in a COI must be identified and accredited with identical Accredited Security Parameters (ASP) (classification levels, compartments, caveats, and mode of operation).

- Connectivity Restrictions. For all connections of an IS to a STU-III/STE data port, the following restrictions apply:
    - Use of the STU-III/STE in the non-secure data mode is prohibited.
    - Use of the STU-III/STE data port feature will be limited to connectivity of a specific set of STU-III/STE terminal units and ISs called a COI.
    - The cable connecting an IS to a STU-III/STE data port must be installed IAW the National TEMPEST technical requirements.

CHAPTER 17 - INTERCONNECTING INFORMATION SYSTEMS

17.1 (U) PURPOSE

This chapter describes policies, issues, and guidance for manual as well as automated processes that can be used to process and move sanitized and collateral information across boundaries of different levels of classification. The primary emphasis in managing information to support the war-fighter is to push information out of the SCI-controlled security domains into collateral security domains.

17.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

17.3 (U) DISCUSSION

Policy requires that SCI information be safeguarded during all phases of operation, processing or storage on ISs. This is required for individual ISs as well as ISs that are connected, particularly when operating at different levels. Different levels refers to two security domains which differ in some component of classification level, including respective compartments, sub-compartments, caveats, control markings or special handling marking. Different levels can also refer to the users (their security clearances, accesses, or need-to-know) of each respective system and the related Levels of Concern (LOC), Protection Level (PL), and the respective technical features implemented within each IS and security domain. When at least one system processes SCI, inter-domain connections will follow the TOP SECRET And Below Interoperability (TSABI) accreditation process. See IC CIO Top Secret/Sensitive Compartmented Information (SCI) and Below Interoperability Policy (TSABI), 7 February 2000

17.3.1 (U) Interconnected Information Systems

Interconnected IS are composed of separately accredited IS's. Whenever separately accredited IS are interconnected, each DAA shall review the security attributes of each system to determine additional security requirements to be imposed. Such a determination will be based on: the technical operating level of each system (LOC/PL); the classification level of the information on each system; or the combination of users who have access to the respective IS. Respective DAAs shall document the interconnection requirements as part of the accreditation for the interconnected systems. Such interconnection determination also applies to support architecture connections, e.g., between networks.

17.3.2 (U) Inter-Domain Connections

When two different ISs are connected and the IS operate at different levels, the connection is an inter-domain connection. Any inter-domain connection, whether between IS or between networks, will comply with DCID 6/3, Section 7.B, Controlled Interface requirements, to provide appropriate confidentiality and integrity adjudication. The accreditation shall follow the TSABI process.

17.3.3 (U) Controlled Interface

The controlled interface requirements may be met by the IS devices themselves, or by a separate device or system added between two domains. Any IS or specific device (or combination) which facilitates the connection between two security domains, IS or networks, is considered a controlled interface. The specific requirements imposed on a controlled interface are highly dependent upon the expected flow of information between the two domains. All controlled interfaces have common requirements to maintain the integrity of the critical processes that control the information flow across the connections. These mandate physical protection of the controlled interface, preventing users from modifying the capabilities of the controlled interface, monitoring usage, and monitoring the interface for failure or compromise. In general, any protocols or services, which are not explicitly authorized, should be denied.

17.3.3.1 (U) One-Way Connections

When information flows in only one direction, the controlled interface requirements may be simplified, but are no less important. A controlled interface used in connection with controlling information flow in only one direction will shut off services and data flow in the reverse direction. The controlled interface may provide automated formatted or pre-determined acknowledge/non-acknowledge messages which do not contain any substantive information to the source IS, without altering the designation as a one-way controlled interface.

17.3.3.1.1 (U) Equal Classification Connections

Connections between ISs or networks of equal classification occur when security domain levels are the same, but are maintained separate for other reasons, e.g. system technical features implemented on the respective IS or the set of users (their security clearances, accesses, or need-to-know).

17.3.3.1.2 (U) Low-to-High Connections

The information being passed from the low side will not have a confidentiality requirement; but the controlled interface will have to maintain the confidentiality of information at the high side from any exposure to the systems or users on the low side. The primary concern of a low-to-high connection is allowing information to flow without significant impairment but with appropriate integrity controls to protect the high side IS and their data. As more unstructured data types are identified for transfer, it becomes more difficult to prevent malicious code from being passed along with the desired information.

17.3.3.1.3 (U) High-to-Low Connections

The primary requirement for high-to-low connections is to protect the confidentiality of information that is not authorized for transfer to the low side. All information being transferred out of a domain, which has classified information that should not be passed across the boundary, will require a process that makes the determination on releasability. The processes that make this determination are called reliable review processes. These processes may be manual (reliable human review), automated (for highly formatted, integrity-wrapped, or reliably labeled information), or a combination depending upon the type and format of the data.

17.3.3.1.4 (U) Other Unequal Classification Level Connections

Sometimes, there is no real high/low relation between two domains, but simply a difference in information where separate data owners on each side of a connection have their own unique

requirements. In this instance, each side is responsible for establishing the confidentiality controls and restrictions for review and release of information to the other side.

17.3.3.2 (U) Dual-Direction Connections

When information is expected to flow in both directions, the requirements of low-to-high, high-to-low, and other equal or unequal level connections must be combined within the implementation of the controlled interface.

17.3.3.3 (U) Multi-Domain Connections

Some controlled interface devices are designed to provide support for connections between more than two domains simultaneously. The implementation for these connections should comply with the requirements for all of the individual combinations of paired connections within the controlled interface device (e.g., three domains have three connection pairs, four domains have six connection pairs, etc.).

17.3.4 (U) Review Procedures

Review procedures for all data transfers are discussed in further detail in 18.3.1.

17.3.4.1 (U) Reliable Human Review

Human review of information has to meet two aspects to be sufficient. First, a review of the information content to validate that it meets criteria for transfer across the domain boundary. Second, a technical review of the information as assembled to ensure that information normally hidden within a presentation is also authorized for transfer across the domain boundary. Any human review process conducted with an IS implements a combination of system capabilities to allow the human to conduct a review of the information. Presentation applications will help the human review data in its presentation form (e.g., a picture looks like a picture). Sometimes these applications will also meet the criteria for technical review by showing data in alternate forms including appended information. If these applications do not have this capability, then other applications may be required to complete technical data reviews. Because a human is interacting with automated processes to conduct reviews, the information being reviewed should have an integrity feature that validates that the review process does not alter the information being reviewed. This added capability is what makes the human review a reliable human review. Integrity and accountability requirements on the reliable human review process will require strong control of the information through the review process and control and accountability for the users associated with the reliable human review.

17.3.4.2 (U) Automated Review

When information is highly formatted, integrity-wrapped, or reliably labeled information, some automated processing may aid a human or may even make the decisions instead of a human. For automation to eliminate the reliable human review, the automated processes need to emulate all activities that would be performed by a human. When the information is not highly formatted, human review will still be required.

17.3.5 (U) Foreign National Access to Systems Processing Classified Information

U.S. Government classified information is not releasable to foreign nationals except as authorized by the U.S. Government.

Data owners can designate their information as releasable to individuals of specific nationalities. The PAA/DAA shall obtain the written permission of all applicable data owners before allowing access by foreign nationals to a system that contains information that is not releasable to individuals of those nationalities.

The decision to allow foreign nationals access to systems that process classified information shall be explicit and shall be in writing. This includes controls over foreign national access or proximity to systems that process NOFORN classified information.

If a proposed IS serves as a controlled interface connection to an IS with foreign national users, the IS must meet controlled interface requirements of DCID 6/3 Chapter 7. The DAA Rep/SCO must ensure that written concurrence for the controlled interface is obtained from data owners and affected DAAs prior to permitting implementation of the connection. Controlled interfaces which connect to an IS that processes SCI information must be accredited through the TSABI process as noted in Chapter 17.

Foreign national ISs may only be allowed in shared SCIF facilities with formal joint approval. Connections between IS are only permitted among systems at the same classification level, upon the approval of the PAA.

CHAPTER 18 - INFORMATION TRANSFER AND ACCOUNTING PROCEDURES

18.1 (U) PURPOSE

This chapter outlines procedures for the transfer of information or software among ISs of different classification levels using information storage media. The procedures are intended to protect the confidentiality of information on the media as well as other data on the end-point IS at different levels, prevent transfers of malicious code (Chapter 10 is germane), and prevent violation of legal copyright or license rights.

18.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

18.3 (U) PROCEDURES

This chapter outlines procedures for the transfer of classified information at varying levels to ISs of different classification levels. For any system that operates with PL-3 and below functionality, media that is placed into that system must be classified at the highest level of information on the system until reviewed and validated. The following address proper classification determination during the access and transfer process. Procedures for data transfers must be approved by the ISSM.

18.3.1 (U) Reliable Human Review of Data

Reliable Human Review is the combination of the data content review, review for hidden data, and integrity controls applied to the information. Human review is a process of validating the classification of data (classification level, compartments, sub-compartments, caveats, control markings or special handling marking) when it is stored or moved from an IS. Human review may be required for validating data classification for hardcopy prints (from systems with less than PL-4 labeling functionality), data being transferred to media, or manual transfers between security domains.

- Human review of information has to meet two criteria to be sufficient: a review of the information content to validate the actual classification level of the data, and a review of embedded or hidden information that is part of the data.
- Human review requires an individual who is knowledgeable of the subject matter to inspect the contents and provide validation of the data classification. This individual has to be able to see the information in its presentation form to make this determination.
- Information in its presentation form does not always show embedded or hidden data. This data may require a different process or application (or tools) to reveal the hidden data for the human review.

- Many users do not realize that some computers often store data on media in fixed length blocks, segments, or tracks. Because data records do not always fill the available space, residual information from memory is appended to the data record. The content of this information is unpredictable and may contain classified or other information from unrelated processes.
- Residual data that exists within information stored in memory may get copied as part of the data whenever it is duplicated.
- There are tools that can aid the human who conducts the review process. Tools (e.g., BUSTER) can aid in the review of large amounts of data. A review of data is more reliable if it includes both a human review and review using tools. Reviews should not rely solely on an automated review. Automated reviews such as tools within guards may be the only authorized exceptions to human review. All automated review processes must be approved by the appropriate DAA.
- Because a human is interacting with automated processes to conduct reviews, the information being reviewed should have an integrity feature so that the review process does not alter the information being reviewed. For example, write protect media before the information review.
- A reliable human review may be a required component of a GUARD or Controlled Interface. Integrity and accountability requirements on the reliable human review process will require strong control of the information and its integrity through the review process, and added controls for accountability for the users associated with the reliable human review.

18.3.2 (U) Media Transfers In/Out of an Organization

All personnel will process outgoing media or report the receipt of media through the ISSM/ISSO or his/her designee before shipment out or use of such media. To ensure the correct classification (including unclassified) and appropriate labeling is being used, conduct reliable human review of 100% of information on the media. During the reliable human reviews, media should be write-protected so that no changes can occur. Identification of incorrect write protection requires installation of correct write protection and then proper conduct (or repetition) of the reliable human review. Virus policy prohibits movement of floppy disks between systems unless appropriate scanning procedures are implemented. If any problems are found, the media is not to be transferred or used, and appropriate reports will be generated and provided to the ISSM/ISSO. If the media is to be subsequently accounted for, make appropriate entries in the organization media accounting system.

18.3.3 (U) Disposition of Excess or Obsolete COTS Software

Software may be reused or released for resale only if:

- The software is still in its original unopened shipping wrapper.
- The user has personal knowledge that the software is not classified and is documented accordingly.

If the user cannot substantiate that the software is not classified, then he/she must ensure classified reutilization within the agency or organization or destruction by approved methods, as appropriate. Do not return the software to the issuing authority if it cannot be reused.

18.3.4 (U) High-to-Low Data Transfer by Media

This section addresses use of media to transfer information from a higher classified system to a lower classified system or a system with a different Accredited Security Parameters (ASP),

including Unclassified. The procedures will differ based on the system capabilities present for different PL levels.

18.3.4.1 (U) PL-3 and Below Functionality

A local SOP must be written to outline the steps to protect the information when transferring data. The following general steps will be identified in the procedures and followed accordingly:

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- The ISSM/ISSO or designee must approve each transfer on a case-by-case basis.
- The media to be used in the process must be new.
- The information to be transferred is placed on the media. Then the media should be write-protected.
- Perform a reliable human review of 100% of the information as stored on the media to verify its classification level.
- Perform scanning of the media for viruses.
- Remove, validate write-protection and mark the media at the appropriate classification level as determined by the human review.
- The media may now be handled as marked.

18.3.4.2 (U) PL-4 and Above Functionality

A local SOP must be written to outline the steps to protect the information when transferring data. The following general steps will be identified in the procedures and followed accordingly:

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- The media to be used in the process must be new.
- Copy the information to the media.
- Perform scanning of the media for viruses.
- Remove, write protect, and mark the media at the appropriate classification level (trusted from the PL-4 and above system).
- The media may now be handled as marked.

18.3.5 (U) Low-to-High Data Transfer by Media

This section addresses use of media to transfer information from a lower classified system, including unclassified, to a higher classified system or a system with a different ASP. A local SOP must be written to outline the steps to protect the media and systems involved when transferring data. One obvious reason for these procedures is to permit unclassified software such as Lotus and dBase to be installed into an IS containing classified information without requiring the media to become classified.

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- The media to be used in the process must be new or an approved transfer disk that has been virus checked.

- Transfer information onto the media.
- Perform scanning of the media for viruses.
- Ensure the transfer media is adequately write-protected if it is to remain classified at the lower level.
- If the write-protect mechanism on the media is securely maintained, the media may remain at its lower classification level (the factory-write protect mechanism on a diskette is adequate).
- If the write protect mechanism is not correctly maintained, the media must be marked and handled at the highest classification level with the most restrictive handling caveats of the information processed by the IS.
- Floppies can be physically write-protected, zip drives can be electronically write-protected and CD/DVDs can remain at the lower classification level when used in read only devices.
- Before transferring information to the higher classified system, perform scanning of the media for viruses.
- Transfer the data from the media to the higher classified IS.
- Following transfer, examine the write-protect device to validate that it is still securely intact.

18.3.6 (U) Demonstration Software

Floppy diskettes and removable hard disks used for demonstrations, with the intent of being returned to a vendor, must be processed on a computer that has never processed or stored classified data. Otherwise, the demonstration media cannot be released back to the vendor and should be destroyed. If returned to the vendor, a fully cleared and indoctrinated individual must verify that the media was used only in an unclassified computer.

CHAPTER 19 - MULTI-POSITION SWITCHES

19.1 (U) PURPOSE

The purpose of this chapter is to provide the policy and procedures outlining the minimum requirements for the management of multi-position switches. This policy applies to all elements that use multi-position switches to share a common keyboard, mouse and monitor between different CPU's. These CPU's may process, store, produce, or transmit information of different classifications, compartments, sub-compartments, code words or releasability.

19.2 (U) SCOPE

This chapter states the policy for Key Board/Video/Mouse (KVM) or Key Board/Monitor/Mouse (KMM) Switches used to connect systems operating at different classification levels, compartments, sub-compartments, caveats, control markings or special handling marking under the cognizant security authority of DIA/NSA including those of contractors. This policy does not restrict the use of these types of devices based on the sensitivity of the information or levels of classification of the data processed on the CPU's that are shared. This policy applies to all individuals who have authorized access to these devices on the systems they use. Not all users are approved for this type of access, and this policy does not provide that approval or countermand in any way any restrictions already placed on the user for the use of these devices.

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

19.3 (U) POLICY

Only KVM switches on the DIA Standard Products List for SCIFs accredited by DIA and KVM switches on the NSA Network Enterprise Solutions (NES) approved products list for SCIFs accredited by NSA shall be used within corresponding SCIFs when sharing a Key Board, Video Monitor or Mouse between CPUs at different classification and/or compartment levels. KVM switches currently in use that do not meet tempest or IS requirements must be replaced with DIA/NSA approved switches. Authorizations are required from the DAAs of the respective systems when using a KVM switch to share the Key Board, Video Monitor, or Mouse. The DAAs are DIA for JWICS, NSA for NSANET, and DISA for NIPRnet and SIPRnet. The use of switchboxes for print services between classification and compartment levels is prohibited. Switchboxes may be used between the same classification and compartment levels for print services.

19.4 (U) RESPONSIBILITIES

19.4.1 (U) DAA Rep

- Ensure all authorizations from DAAs of respective systems are obtained.

19.4.2 (U) ISSM

- Maintain the KVM Switch User Agreements files.
- The ISSM will verify that the user has the necessary training and complies with the requirements for the introduction and use of multi-position switches.

19.4.3 (U) ISSO/System Administrator

- Ensure that the Configuration Management Board (CMB) approves the systems.
- Ensure that the systems are installed correctly and meet all TEMPEST Standards.
- Ensure the desktop banners, backgrounds, and screen locks have the proper classification banner.
- Ensure the KVM is documented and approved in all pertinent SSP/SSAAs.

19.4.4 (U) User

- Protect the Information System and KVM in your area.
- Report any spillage of classified information IAW the JDCSISSS.
- Safeguard and report any unexpected or unrecognized computer output, including both displayed and printed products IAW JDCSISSS.
- Use different passwords on each system connected through a KVM.
- Ensure that each systems screen lock displays the classification level and that a password is required to regain entry to the system.
- Ensure that the systems screen lock is invoked if the system is left unattended or if there is a 15-minute period of inactivity for each system.
- Responsible for marking/maintaining magnetic media IAW Chapter 12 of JDCSISSS.

19.5 (U) IS REQUIREMENTS

The introduction and use of multi-position switches in a SCI environment presents a moderate degree of risk to classified or sensitive information and systems. Therefore, all users will be responsible for the management of these devices. To minimize the risk of inadvertently entering information onto the wrong network, the following requirements must be met. Authorization of the KVMs must be documented within all respective certification and accreditation documents.

- Port Separation. The switch must be used with ports one and two for one classification level (i.e. unclassified and/or secret) and ports three and four for higher classification levels (i.e. JWICS and NSANet).
    - For example and additional protection using the approved 4-port switchbox for three different classifications, use Port 1 for Unclassified, Port 2 for Secret and Port 4 for SCI.
- Labels. All information systems components must be labeled IAW DCID 6/3, Paragraph 8.B.2 (a and b). All switch positions, cables, and connectors must be clearly marked with the appropriate classification labels.
- Desktop Backgrounds. To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the

banner background will be in a solid color that matches the classification (SCI - yellow, Top Secret - orange, Secret - red, Confidential - blue, Unclassified - green). When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

- Screen Locks. Screen Lock applications must display the maximum classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.
- Smart Keys/Permanent Storage Medium. Systems using KVM switches must not employ "smart" or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications.
- Hot Key Capability. Switches that support "Hot-Key" capability to switch, toggle or otherwise affect the switching between CPUs are prohibited.
- Scanning Capability. Switches with the ability to automatically scan and switch to different CPUs are prohibited.
- Wireless or Infrared Technology. Systems using KVM switches must not use keyboards or mice with wireless or infrared technology
- Unique Password Requirement. At a minimum, users must ensure that they use different/unique passwords for each system connected through a multi-position switch. Whenever possible, system administrators should employ different logon USERIDs to help users further distinguish between the systems.
- Data Hierarchy. Data of a higher classification must not be introduced to a system of a lower classification.
- Security CONOPS. A site with a requirement for multi-position switches must include the KVM procedures within the site's SECONOPS. The approval authority will be the Site ISSM.
- Training. ISSMs/ISSOs/Supervisors will ensure user training and compliance to the requirements associated with the introduction and use of multi-position switches.
- TEMPEST. Blanket approval to install KVM switches is granted within DIA accredited SCIFs located within the US and meeting NSTISSAM TEMPEST/2-95A, 3 Feb 00, recommendation "I" (having 100 meters of inspectable space) as defined by the SCIF's TEMPEST accreditation document from DIA/DAC-2A. Blanket approval to install KVM switches is granted within NSA accredited SCIFs located within the US and meeting NSTISSAM TEMPEST/2-95A, 3 Feb 00, Zones C and D having more than 100 meters of inspectable space. Prior approval is required for overseas facilities and all other recommendations.

19.6 (U) Procedures for LOGON/Switching Between Systems

19.6 1 (U) Logging on to systems

- Identify the classification of the system currently selected.
- Use the login and password appropriate to that system.
- Verify the classification of the present system by checking the classification label.
- Begin processing.

19.6.2 (U) Switching between systems

- Select desired system with the multi-position switch.
- Verify the classification of the present system by checking the classification label.
- Begin processing at the new classification level.

EXCEPTIONS. Any exception to this policy requires approval of the DAA Rep responsible for the Certification/accreditation of systems in your SCIF.

19.7 (U) KVM SWITCH USER AGREEMENT

The user agreement (Figure 19-1) documents training and certification for personnel using the KVM switch.

KVM USER AGREEMENT FORM

1. (U) KVM SWITCH USER AGREEMENT. The user agreement documents training and certification for personnel using the KVM switch.

1.1. (U) Procedures for LOGIN and Switching Between Systems. This process must be performed for each switch between systems. When the DoDIIS system is not selected, it is required to be screenlocked.

1.1.1. (U) Logging onto a System.

- Identify the classification of the system currently selected
- Use the login and password(s) appropriate to that system
- Verify the classification of the present system by checking the classification label
- Begin Processing

1.1.2. (U) Switching Between Systems.

- Screenlock the system you are currently working on.
- Select desired system with the KVM switch.
- Enter your user id and password to deactivate the screen lock.
- Verify the classification of the present system by checking the classification label.

1.1.3. (U) Logging Off of a System.

- Close all applications processing on the active system
- Logout of the system when processing in no longer required on the system
- Logout of system at the end of duty day

1.2. (U) A weekly inspection of tamper seals (if any) will be performed by the user.

1.3. (U) Any suspected tampering and/or mishandling of KVM will be reported to your site ISSM.

Printed Name of User

_____

Signature _____ Date _____

The above individual has received the necessary training and has complied with the requirements for application and use of KVM switches

Printed Name of ISSM

_____

Signature _____ Date _____

Figure 19.1 (U) Kvm Switch User Agreement Form.

CHAPTER 20 – COLLABORATIVE COMPUTING

20.1 (U) PURPOSE

The purpose of this chapter is to provide guidance and procedures to for use of video cameras and microphones on information systems within SCIFs. This guidance applies to all organizations using video cameras and microphones on information systems for collaborative computing. This guidance also applies regardless of the sensitivity of the information or levels of classification for which the video cameras/microphones are being used.

20.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

20.3 (U) IMPLEMENTATION PROCEDURES

If not correctly configured and controlled, collaborative computing technologies can allow an unauthorized user to see and hear national security information and material at another user's workstation area that they may not be cleared for. This policy establishes the minimum technical and procedural controls that must be in place to limit these risks.

20.3.1 (U) Collaborative Computing Activation

Collaborative computing mechanisms shall not be remotely activated, nor may they have any auto-answer capabilities that automatically activate the video and audio recording/transmitting devices. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop shall be required to take an explicit action to turn on the camera and microphone). Remote activation of a user's camera or microphone is prohibited.

- Collaborative computing mechanisms that provide video and/or audio conference capabilities shall provide a clear visible indication that the video and audio mechanisms are operating to alert SCIF personnel when recording or transmitting.
- While conducting a collaborative computing session, the user shall take all reasonable measures to ensure that no sensitive information is inadvertently made either auditibly or visually accessible to the collaborative computing mechanism. This includes advising all personnel in the immediate area that the collaborative computing mechanism will be operating as well as sanitizing any other sensitive material/system that may be in view of the video recording/transmitting equipment.
- Once the collaborative session is completed, the user shall immediately take an explicit action to disconnect/terminate the collaborative computing mechanism.
- Users shall not leave the workstation unattended while a peer-to-peer collaborative computing mechanism is in progress.

20.3.2 (U) Video cameras/microphones connected to SCI information systems

- Camera(s) must have a device or clear visible display that notifies the user when it is in use (e.g., light).
- Camera(s) will be turned off and lens will be covered with an opaque covering, when camera is not in use.
- Microphone(s) should have a push to talk button (implemented in hardware or software), but must have a mute or hold capability (e.g., on/off switch).
- Use of cameras/microphones must have written approval from the site ISSM and all collaborative computing devices must be identified on the facility's baseline.
- Desktop level collaborative computing mechanisms must use a headset. If external loud speakers/amplified sound are used, the system speakers must be installed within a closed room with walls that meet the requirements of DCID 6/9, of sound transmission class (STC) 50 or better, (sound group 4).

20.3.3 (U) Video cameras/microphones connected to collateral/unclassified information systems

- Cameras must be placed in an enclosed area with a door that is acoustically isolated from the other SCI discussion areas.
- No systems/documents/media of greater classification may be displayed or in view of the camera(s).
- Camera(s) must have a device or clear visible display that notifies the user when it is in use (e.g. light).
- Camera lens will be covered with an opaque covering, when the camera is not in use.
- A classification sign will be placed on door when camera or microphone is in use.
- Microphone(s) should have a push to talk button (implemented in software or hardware), but must have a mute or hold capability (e.g., on/off switch).
- Use of cameras/microphones must have written approval from the site ISSM and all collaborative computing devices must be identified on the facility's baseline.
- Unclassified video teleconferencing centers (VTC) and/or like video/audio recording equipment must be deactivated and disconnected when not in use.

20.3.4 (U) Collaborative Computing Approval

Any multi-classification collaborative computing mechanisms, VTC or like systems that have video and/or audio capability integrated into one system must be previously approved by the DIA certified tempest technical authority (CTTA). Approval may be requested by submitting appendix "j" of DoD 5105.21-M-1 to DIA/DAC-2A for review.

20.3.5 (U) Responsibilities

- ISSM:
- Verify that the user has the necessary training and complies with the requirements for the introduction and use of video cameras/microphones.
- ISSO/system administrator:
- Ensure that the configuration management board approves the cameras/microphones.

- Ensure that the video cameras/microphones are installed correctly and meet all TEMPEST standards, (i.e., refer to your facilities TEMPEST accreditation for the specific red/black installation guidance and outlined in NSTISSAM TEMPEST 2-95(a) Dtd: 03 Feb 2000 (U//FOUO).
- User:
- Protect the information system in your area;
- Ensure camera/microphone is off when not in use;
- Ensure cover is placed over lens of camera when not in use;
- Report any violation of this policy to the site ISSM as a security incident.

CHAPTER 21 - CLEARING, SANITIZING, AND RELEASING COMPUTER COMPONENTS

21.1 (U) PURPOSE

The purpose of this chapter is to provide guidance and procedures to clear and sanitize magnetic storage media that is no longer useable, requires transfer, or should be released from control. These procedures apply to all ISs containing electronic, electromagnetic, electrostatic, or magnetic storage media. For clarification, Magnetic storage media is considered to be any component of a system that, by design, is capable of retaining information without power.

21.2 (U) SCOPE

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

21.3 (U) RESPONSIBILITIES

The ISSM is responsible for the security of all ISs and media assigned to the organization and under his/her purview. To protect these assets, he/she must ensure the security measures and policies contained within this chapter are followed. Additionally, the ISSM will publish supplemental organizational procedures (SOPs, etc.), if needed, to implement the requirements herein.

21.4 (U) Review of Terms

To better understand the procedures contained herein, it should be understood that overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with declassification. The following are definitions:

- Clearing. Clearing is the process of removing information from a system or the media to facilitate continued use and to preclude the IS from recovering previously stored data. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. Clearing can be accomplished by overwriting or degaussing.
- Sanitizing (Also purging). Sanitizing is the process of removing information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. In general, laboratory techniques cannot retrieve data that has been sanitized/purged. Sanitizing may be accomplished by degaussing.
- Destruction. Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data.
- Declassification. Declassification is an administrative process used to determine whether media no longer requires protection as classified information. The procedures for declassifying media require DAA Rep or SCO approval.

- Periods Processing. Provided the sanitization procedures between each protection level segment have been approved by the DAA Rep/SCO based on guidelines from the data owner(s) or responsible official(s), the system need meet only the security requirements of each processing period, while in that period. If the DAA Rep/SCO approves the sanitization procedures for use between periods, the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitization procedures shall be detailed in the SSAA/SSP.

***NOTE:** Periods processing will not be approved for NSA accredited system.

21.5 (U) PROCEDURES

The procedures contained below meet the minimum-security requirements for the clearing, sanitizing, releasing, and disposal of magnetic media as well as guidance for other types of information storage media. These procedures will be followed when it becomes necessary to release magnetic media, regardless of classification, from SCI channels. Overwriting can not sanitize media that has ever contained SCI, other intelligence information, or Restricted Data. Such media must be degaussed before release.

21.5.1 (U) Overwriting Media

Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing. However, the effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. Software overwrite routines may be corrupted by hostile computer viruses. Overwriting is not an acceptable method to declassify media.

- Overwriting Procedure. The preferred method to clear magnetic disks is to overwrite all locations with a pseudo-random pattern twice and then overwrite all locations with a known pattern.
- Overwrite Verification. Overwrite procedures must be verified by the ISSM or his/her designee.

21.5.2 (U) Degaussing Media

Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

Magnetic media is divided into four types (I, II, IIA, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained prior to executing any degaussing procedure.

21.5.2.1 Types of Degausser

The individual performing the physical degaussing of a component must ensure that the capability of the degausser meets or exceeds the coercivity factor of the media, and that the proper type of degausser is used for the material being degaussed. The four types of degaussers are:

- Type I. Used to degauss Type I media (i.e., media whose coercivity is no greater than 350 Oersteds [Oe]).

- Type II. Used to degauss Type II media (i.e., media whose coercivity is no greater than 750 Oe).
- Type IIA. Used to degauss Type IIA media (i.e., media whose coercivity ranges from 751 to 900 Oe).
- Type III. Used to degauss Type III media (i.e. media whose coercivity ranges from 901 to 1700 Oe). Currently, there are no degaussers that can effectively degauss all Type III media. Some degaussers are rated above 901Oe, and their specific approved rating will be determined prior to use.

21.5.2.2 (U) Degausser Requirements

Refer to the current issue of the National Security Agency (NSA) Information Systems Security Products and Services Catalogue (Degausser Products List Section), for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specification. National specifications provide a test procedure to verify continued compliance with the specification.

21.5.2.3 (U) Use of a Degausser

Once a degausser has been purchased and has become operational, the gaining organization must establish a SOP explaining how it will be used. The degausser must be certified annually.

21.5.3 (U) Sanitizing Media

Tables 21-1 and 21-2 provide instructions for sanitizing data storage media and system components.

Table 21.1. (U) Sanitizing Data Storage Media

MEDIA TYPE	**PROCEDURE(S)**
Magnetic Tape	
Type I	a or b
Type II,IIA	b
Type III	Destroy
Magnetic Disk Packs	
Type I	a or b
Type II,IIA	b
Type III	Destroy
MEDIA TYPE	**PROCEDURE(S)**
Magnetic Disks	
Floppies	a or b, then Destroy

Bernoullis	Destroy
Removable Hard Disks	a or b
Non-Removable Hard Disks	a or b
Optical Disks	
Read Only (including CD-ROMs)	Destroy
Write Once, Read Many (WORM)	Destroy
Read Many, Write Many	Destroy
PROCEDURES	
These procedures will be performed or supervised by the ISSO.	
a. Degauss with a Type I degausser. See 21.4.3.2.	
b. Degauss with a Type II, IIA degausser. See 21.4.3.2.	

Table 21.2. (U) Sanitizing System Components

TYPE OF COMPONENT	**PROCEDURE(S)**
Magnetic Bubble Memory	a or b or c
Magnetic Core Memory	a or b or d
Magnetic Plated Wire	d or e
Magnetic-Resistive Memory	Destroy
SOLID STATE MEMORY COMPONENTS	
Dynamic Random Access Memory (DRAM) (Volatile)	e and i
if RAM is functioning	d, then e and i
if RAM is defective	f, then e and i
Static Random Access Memory (SRAM)	j
Programmable ROM (PROM)	Destroy (see h)
Erasable Programmable ROM (EPROM/UVPROM)	g, then c and i
Electronically Erasable PROM (EEPROM)	d, then i
Flash EPROM (FEPROM)	d, then i
PROCEDURES	
These procedures will be performed or supervised by the ISSO.	

a. Degauss with a Type I degausser.
b. Degauss with a Type II, IIA degausser.
c. Overwrite all locations with any random character.
d. Overwrite all locations with a random character, a specified character, then its complement. (Contact vendor for specific erase procedures, usually accomplished via the command prompt/MS-DOS prompt)
e. Remove all power, including batteries and capacitor power supplies from RAM circuit board.
f. Perform three-power on/off cycles (60 seconds on, 60 seconds off each cycle, at a minimum).
g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
h. Destruction required only if ROM contained a classified algorithm or classified data.
i. Check with the ISSPM/DAA Rep/SCO to see if additional procedures are required.
j. Store a random unclassified test pattern for a time period comparable to the normal usage cycle.

21.5.4 (U) Destroying Media

Data storage media will be destroyed IAW DAA/DAA Rep/SCO approved methods.

21.5.4.1 (U) Expendable Item Destruction

Expendable items (e.g., floppy diskettes and hard drives) are not authorized for release and reuse outside of the SCI community after they have been degaussed (Table 21.1). If these items are damaged or no longer deemed usable, they will be destroyed. When destroying, remove the media (magnetic mylar, film, ribbons, etc.) from any outside container (reels, casings, hard cases or soft cases, envelopes, etc.) and dispose of the outside container in a regular trash receptacle. Cut the media into pieces (a crosscut chipper/shredder may be used to cut the media into pieces) and then burn all pieces in a secure burn facility or pulverize to 2.5mm (3/16-inch) specification. If the Environmental Protection Agency (EPA) does not permit burning of a particular magnetic recording item, it will be degaussed, cut into pieces (a chipper/shredder preferred) and disposed of in a regular trash receptacle.

Note: Use of a burn bag does not necessarily mean that organizations actually burn. Many organizations have pulverization facilities that handle all burn bags.

21.5.4.1.1 (U) Shipping Instructions

Below are the shipping instructions for destruction of other classified items to include floppy discs, typewriter ribbons, magnetic tapes, hard drives that have been removed from the reels, film, viewgraphs, chips, circuit boards, exterior cases and paper. Paperwork required is either an SF153 Destruction Form or a DD1149 (shipping document). POC is at NSA LL24, commercial (301) 688-6136/DSN 644-6136 (NSTS 972-7248), Suite 6875;

- COMSEC MATERIAL, send by regular mail to:
- DIRNSA ATTN: LL24
- Account #889999
- Fort Meade, MD 20755-6000

- NON-COMSEC MATERIAL CLASSIFIED UP TO AND INCLUDING SECRET, send by regular mail to:

  National Security Agency

  ATTN: CMC – LL24 - Suite 6890

  9800 Savage Road

  Fort George G. Meade, MD 20755-6890

- NON-COMSEC MATERIAL CLASSIFIED HIGHER THAN SECRET, send by DCS to:
- 449563 - BA20
- Film Destruction Facility

21.5.4.2 (U) Destruction of Hard Disks

Hard disks are expendable items and are not authorized for release and reuse outside of the SCI community. Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If hard disks are damaged, or no longer deemed usable, they will be degaussed and then destroyed. If the platter(s) of the defective unit can be removed and the removal is cost effective, then destruction of a hard disk consists of dismantling the exterior case and removing the platter from the case then degaussing the platter. Techniques that remove the recording surface (grinding or chemical etching the oxide surface) prior to disposal do not enhance security and are unnecessary. They may be disposed of by using approved procedures for the destruction or disposal of unclassified metal waste.

21.5.4.2.1 (U) Shipping Instructions

Below are the shipping instructions for destruction of magnetic media, including cassette tapes, videotapes, hard disks, optical disks (including CDs) and magnetic tapes on reels. Paperwork required is either a DD1149 (shipping document) or 1295A (transmittal of classified material document). POC is at NSA LL24, (301) 688-6136 DSN 644-6136 (NSTS 977-7248).

- CLASSIFIED UP TO AND INCLUDING SECRET, send by regular mail to:

  National Security Agency

  9800 Savage Road

  Fort George Meade, MD 20755-6875

  SAB-3, Suite 6875

  Attn: CMC, Degaussing

- CLASSIFIED HIGHER THAN COLLATERAL SECRET, send via Defense Courier Service (DCS) to:

  449276-BA21

  DIRNSA, FT MEADE

  Degaussing

- CLASSIFIED EQUIPMENT UP TO AND INCLUDING SECRET, send by regular mail:

  National Security Agency

9800 Savage Road

Fort George Meade, MD 20755-6632

SAB-4, Suite 6632

Attn: LL23 Cleansweep

- CLASSIFIED EQUIPMENT HIGHER THAN COLLATERAL SECRET, send via Defense Courier Service (DCS) to:

  449276-BA21

  DIRNSA, FT MEADE

  CLEANSWEEP

Note: Phone POC for equipment questions, (301) 688-6776 or (NSTS) 977-7183.

21.5.4.3 (U) Destruction of Disk Packs

Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If disk packs are damaged, or no longer deemed usable, they will be degaussed and then destroyed. Techniques that remove the recording surface (grinding or chemical etching the oxide surface) prior to disposal do not enhance security and are unnecessary. They may be disposed of by using approved procedures for the degauss and destruction or disposal of unclassified metal waste.

21.5.4.4 (U) Optical Storage Media Destruction

Optical mass storage, including compact disks (CD, CDE, CDR, CDROM), optical disks (DVD), and magneto-optical disks (MO) shall be declassified by means of destruction. Optical media shall be destroyed by burning, pulverizing, or grinding the information bearing surfaces. When material is pulverized or ground, all residue must be reduced to pieces sized 0.25mm or smaller. Burning shall be performed in an approved facility certified for the destruction of classified materials; residue must be reduced to white ash.

21.5.5 (U) Malfunctioning Media

Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the ISSO/SA. The ISSO/SA will coordinate the repair or destruction of the media with the ISSM and responsible DAA Rep/SCO. If the hard drive is under a warranty that requires return of the hard drive, dismantle the hard drive and return the case but do not send the platter to the manufacturer.

21.5.6 (U) Release of Memory Components and Boards

Prior to the release of any malfunctioning components proper coordination, documentation, and written approval must be obtained by the ISSM. This section applies only to components identified by the vendor or other technically-knowledgeable individual as having the capability of retaining user-addressable data; it does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this chapter, a memory component is considered to be the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release (See Table

21-2). Memory components are specifically handled as either volatile or non-volatile, as described below.

21.5.6.1 (U) Volatile Memory Components

Memory components that **do not** retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system, are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only IAW procedures developed by the ISSM, or designee, and documented in the SSAA/SSP. A record must be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.

21.5.6.2 (U) Non-volatile Memory Components

Components that **do** retain data when all power sources are discontinued are nonvolatile memory components. Some nonvolatile memory components (e.g., Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM)) and their variants that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components (e.g., removable/non-removable hard disks) may be released after successful completion of the procedures outlined in Table 21-2. Failure to accomplish these procedures will require the ISSM, or designee, to coordinate with the DAA Rep/SCO to determine releasability.

21.5.6.3 (U) Other Non-volatile Media

The following non-volatile media could possibly retain data when all power sources are discontinued.

21.5.6.3.1 (U) Visual Displays

A visual display may be considered sanitized if no sensitive information is etched into the visual display phosphor. The ISSO should inspect the face of the visual display without power applied. If sensitive information is visible, destroy the visual display before releasing it from control. If nothing is visible, the ISSO/SA shall apply power to the visual display; then vary the intensity from low to high. If sensitive information is visible on any part of the visual display face, the visual display shall be destroyed before it is released from control.

21.5.6.3.2 (U) Printer Platens and Ribbons

Printer platens and ribbons shall be removed from all printers before the equipment is released. One-time ribbons and inked ribbons shall be destroyed as sensitive material. The rubber surface of platens shall be sanitized by wiping the surface with alcohol.

21.5.6.3.3 (U) Laser Printer Drums, Belts, and Cartridges

- Laser printer components containing light-sensitive elements (e.g., drums, belts, and complete cartridges) shall be sanitized before release from control.
- Elements containing intelligence information shall be sanitized IAW the policy contained in the DCID 6/9.
- Used toner cartridges from properly operating equipment that properly completed the last printing cycle may be treated, handled, stored and disposed of as UNCLASSIFIED.

- When a laser printer does not complete a printing cycle (e.g., a paper jam or power failure occurs) completing a subsequent print cycle before removal of the cartridge is sufficient to wipe residual toner from the cartridge drum.
- If the toner cartridge is removed without completing a print cycle, inspect the cartridge drum by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient action to wipe off residual toner material present.
- After completing actions for incomplete print cycles, the toner cartridge may be treated, handled, stored and disposed of as UNCLASSIFIED.

21.5.7 (U) Clearing Systems for Periods Processing

Systems authorized for periods processing must be cleared of any information that is not authorized between the different defined periods of mode/level of operation. All system components must be cleared IAW guidance of this chapter.

- Most systems will have volatile memory components. Removing power (turning the system off) can clear these components.
- Some systems have removable media designed to save time and be more convenient for changing between modes/levels (e.g., this avoids having to overwrite the media and re-install all of the software including complex operating system software). The IS should be shut down before the removable media is exchanged.
- Nonvolatile memory components, which are significant components of a system, could retain information between the periods. When relying on removable media, the system should have no significant nonvolatile memory components that could contain unauthorized information remaining within the system.
- Any system approved for periods processing will be prohibited from containing nonvolatile memory or a fixed hard drive.
- For example, a PL-2 system with a removable hard drive “for data” which is interchanged between periods is not sufficient if a permanent hard drive remains inside the IS with “just the operating system”. The PL-2 system does not provide sufficient controls to trust against unauthorized information inadvertently being stored to the operating system hard drive.

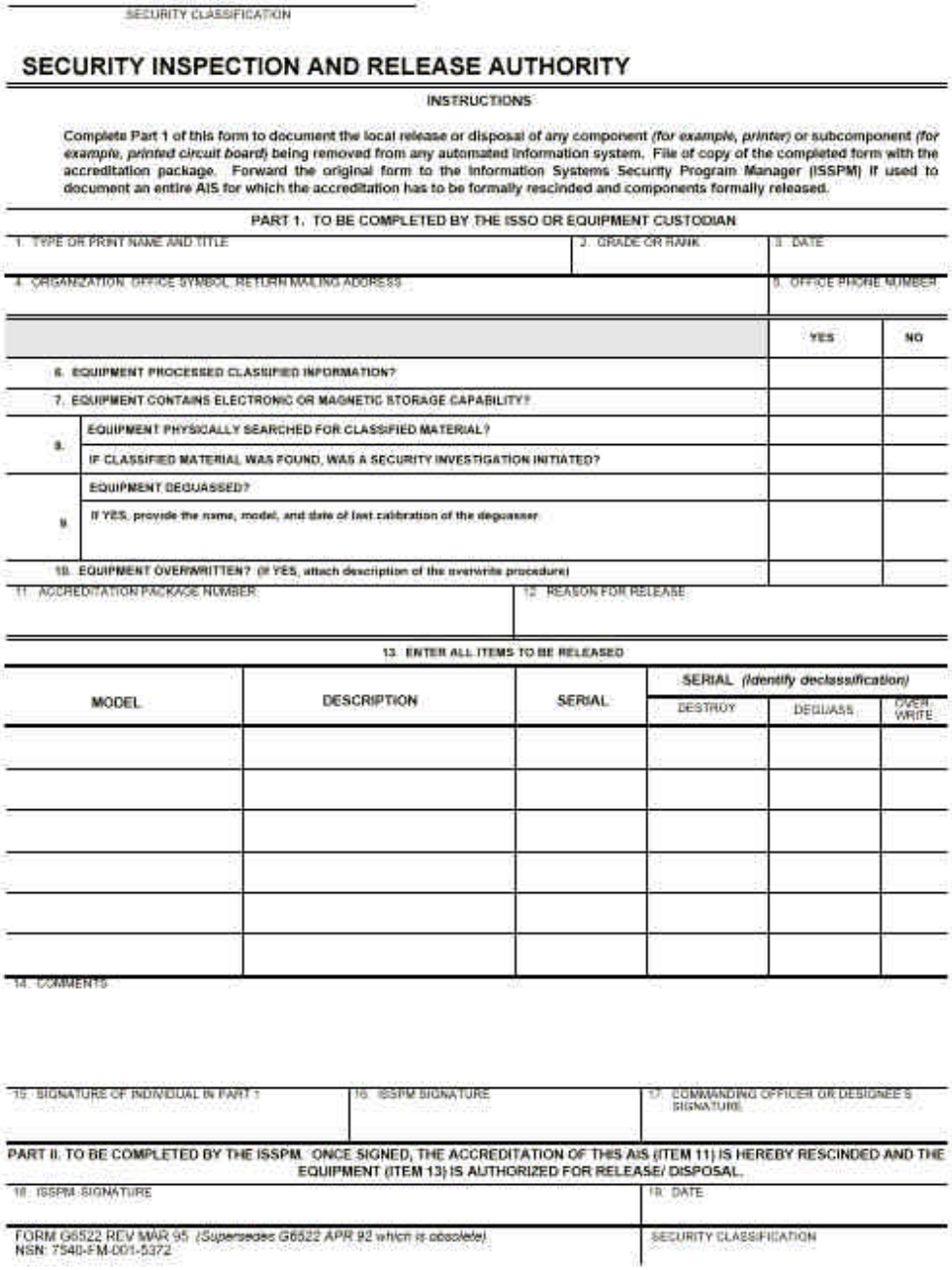
21.5.8 (U) Release of Systems and Components

The ISSM, or designee, shall develop equipment removal procedures for systems and components and these procedures shall be stated in the SSAA/SSP. When such equipment is no longer needed, it can be released if:

- It is inspected by the ISSM, or designee. This inspection will assure that all media, including internal disks, have been removed or sanitized.
- A record is created of the equipment release indicating the procedure used for sanitization and to whom the equipment was released. The record of release shall be retained for a period prescribed by the DAA Rep/SCO.
- Procedures specified by the DAA Rep/SCO are used.

21.5.8.1 (U) Documenting IS Release or Disposal

The NSA/CSS Form G6522, shown in Figure 21.1, or similar form/documentation, will be used to document the local release or disposal of any IS or processing component.



SECURITY CLASSIFICATION

SECURITY INSPECTION AND RELEASE AUTHORITY

INSTRUCTIONS

Complete Part 1 of this form to document the local release or disposal of any component *(for example, printer)* or subcomponent *(for example, printed circuit board)* being removed from any automated information system. File of copy of the completed form with the accreditation package. Forward the original form to the Information Systems Security Program Manager (ISSPM) if used to document an entire AIS for which the accreditation has to be formally rescinded and components formally released.

PART 1. TO BE COMPLETED BY THE ISSO OR EQUIPMENT CUSTODIAN

1. TYPE OR PRINT NAME AND TITLE	2. GRADE OR RANK	3. DATE
4. ORGANIZATION, OFFICE SYMBOL, RETURN MAILING ADDRESS		5. OFFICE PHONE NUMBER

	YES	NO
6. EQUIPMENT PROCESSED CLASSIFIED INFORMATION?		
7. EQUIPMENT CONTAINS ELECTRONIC OR MAGNETIC STORAGE CAPABILITY?		
8. EQUIPMENT PHYSICALLY SEARCHED FOR CLASSIFIED MATERIAL?		
8. IF CLASSIFIED MATERIAL WAS FOUND, WAS A SECURITY INVESTIGATION INITIATED?		
9. EQUIPMENT DEGAUSSED?		
9. If YES, provide the name, model, and date of last calibration of the degausser		
10. EQUIPMENT OVERWRITTEN? (If YES, attach description of the overwrite procedure)		

11. ACCREDITATION PACKAGE NUMBER	12. REASON FOR RELEASE

13. ENTER ALL ITEMS TO BE RELEASED

MODEL	DESCRIPTION	SERIAL	SERIAL *(Identify declassification)*		
			DESTROY	DEGAUSS	OVER WRITE

14. COMMENTS

15. SIGNATURE OF INDIVIDUAL IN PART I	16. ISSPM SIGNATURE	17. COMMANDING OFFICER OR DESIGNEE'S SIGNATURE

PART II. TO BE COMPLETED BY THE ISSPM. ONCE SIGNED, THE ACCREDITATION OF THIS AIS (ITEM 11) IS HEREBY RESCINDED AND THE EQUIPMENT (ITEM 13) IS AUTHORIZED FOR RELEASE/ DISPOSAL.

18. ISSPM SIGNATURE	19. DATE
FORM G6522 REV MAR 95 *(Supersedes G6522 APR 92 which is obsolete)* NSN: 7540-FM-001-5372	SECURITY CLASSIFICATION

Figure 21.1. (U) Sample NSACSS Form G6522

CHAPTER 22 - INFORMATION SYSTEMS (IS) AND NETWORK SECURITY SELF-INSPECTION AID

22.1 (U) PURPOSE

The purpose of this chapter is to provide an aid for the inspection, certification, and accreditation of SCI ISs. The checklist is based upon the criteria contained in this document and other applicable DoD security regulations/directives. This checklist can be used as follows:

- To inspect IS operations periodically throughout their life cycle
- To inspect organizational IS security program
- Incorporated as part of an organization's self-inspection program
- In preparation for formal inspections, IS certifications and accreditations

22.2 (U) SCOPE

This aid is effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	NO
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

22.3 (U) APPLICABILITY

This checklist is applicable to those systems and security programs that support DoD SCI operations. The ISSM/ISSO should periodically complete the checklist (recommended annually).

22.4 (U) PROCEDURES

The completion of this self-inspection checklist is basically self-explanatory and may be locally reproduced to meet the self-inspection and IS certification and accreditation requirements of an organization.

Table 22.1 (U) IS AND NETWORK SECURITY SELF-INSPECTION CHECKLIST

IS AND NETWORK SECURITY SELF-INSPECTION CHECKLIST			
SECTION A – IS SECURITY PROGRAM MANAGEMENT & DOCUMENTATION			
	YES	**NO**	**NA**
1. Is the IS Security Program being supported by supervisors and senior managers?			
2. Has an IS and Network Security Program been established?			
3. Is the ISSM appointed in writing and has a copy of the appointment letter been forwarded to to the Designated Accrediting Authority (DAA) /DAA Representative (REP)/Service Certifying Organization (SCO), and does the ISSM maintain a copy of the appointment letter on file at the unit? **[JDCSISSS 1.5.8]**			
a. Has an IS Security Training Program been established to ensure DoD certification of SAs, ISS personnel and IS users? **[JDCSISSS 1.5.8]**			
b. Has the ISSM attended training (Information Security)**? [JDCSISSS 1.5.8]**			
c. Has the ISSM ensured all ISSO's received the necessary Technical & Security training to carry out their duties? (OIAC 2225, or the Department of Defense Intelligence Information Systems (DoDIIS) Site ISSM Course or equivalent course) **[JDCSISSS 1.5.8]**			
d. Are signs posted throughout the organization with the names and phone numbers of the Security Officers?			
e. Has a self-inspection of the organization IS and Network Security Program been conducted?			
f. Have identified deficiencies been documented?			
g. Does the responsible authority review self-inspection reports to ensure follow-up actions are taken to correct all identified deficiencies?			
h. Have all identified deficiencies been corrected?			
4. Are assistance visits conducted to assist subordinate units (if any) in the development of their IS & Network Security Programs?			
5. Are appropriate IS security regulations/policy documents being maintained, and are they accessible to the ISSM, ISSO, SA and system users? Are they on file and used effectively to manage the organization's IS & Network Security Program?			
a. HQs-level advisory messages. Is there a procedure in place to ensure that all Bulletins/IAVAs (or Defense Information Systems Agency's (DISA) Automated System Security Incident Support Team (ASSIST) and the Service's Computer Emergency/Incident Response Team (CERT/CIRT).) are reviewed and applied as necessary**? [JDCSISSS 1.5.8]**			

b. Policy letters and directives.			
c. SSAA/SSPs and any associated approval to operate documentation.			
d. SCIF Accreditation Documentation on each SCIF on file?			
e. If your Site/SCIF contains other organizations, are there Memorandums of agreement (MOA) in place detailing the nature of IS accreditation support provided by each organization**? [DOD 5105.21-M-1, Chapter 1, para F.4.f]**			
f. If "Guest" systems are located within the SCIF, does the ISSM have approved documentation for approval to operate? **[JDCSISSS 4.6.1]**			
g. Are current Physical Security accreditation's for each SCIF on file?			
h. Is the site CONOPs current and being followed by your Site/SCIF? **[DCID 6/3 4.B.1.c(1)(b) and DCID 6/3 9.D.3.b.2]**			
i. Risk analysis and vulnerability reports.			
j. TEMPEST checklists, certificates, and waivers, if applicable, for all installed ISs? **[JDCSISSS 5.5.2]**			
k. Self-inspection reports and appropriate follow-up actions.			
6. Are the results of security incidents/violations investigated, reported IAW applicable regulations, and reviewed to determine whether changes to IS policy/procedures are required?			
a. Are all personnel aware of their responsibilities in reporting IS incidents and violation?			
SECTION B - ACCREDITATION AND CERTIFICATION			
7. Has a System Security Authorization Agreement [SSAA]/ Systems Security Plan [SSP]) been:			
a. Does the ISSM (or equivalent) review and endorse all IS accreditation/certification support documentation packages? **[DCID 6/3 2.B.6.c.6 and JDCSISSS 1.5.8]**			
b. Are the accreditation packages in the prescribed format and submitted on ALL systems? **[DCID 6/3 Chapter 9.C.3 and JDCSISSS Chapter 3 & 4]**			
c. Is a program/procedure in place ensuring re-certification of each accredited IS is completed upon its three year anniversary? **[DCID 6/3 9.D.7.b and JDCSISSS 3.4.5]**			
d. Does the accreditation package submitted have the appropriate classification level? **[JDCSISSS 3.5.6 & 4.7.1]**			
e. Is the accreditation process included in annual IS and network security training? **[JDCSISSS 6.3.9]**			
f. Are IS connectivity drawings available? **[DCID 6/3 2.B.7.c(7)]**			
g. If Site-Based, do you have current accreditations from the appropriate Designated Approval Authority (DAA) for all SAP/SAR, collateral and unclassified systems within your site? **[DCID 6/3 2.B.6.c(8)]**			

h. If not Site Based do you have current accreditations for all systems within your Site/SCIF?			
i. If Site-Based, is the "Change" block of the Baseline used to track changes to the accredited Baseline?			
j. Developed for the Information Systems?			
k. Properly coordinated within the organization (ISSM, ISSO/SA, Physical Security personnel, TEMPEST Officer, etc.)? {TEMPEST change ICW Chapter 5?}			
l. Reviewed by the ISSM for appropriate action?			
m. A file copy maintained by ISSM/ISSO?			
n. Has the ISSM/ISSO coordinated the accreditation documentation with their CCB?			
o. Is appropriate accreditation/IATO documentation maintained by ISSM/ISSO for each IS?			
p. Have all ISs been certified and accredited prior to operation or an IATO granted?			
q. Forwarded to the appropriate DAA/DAA Rep/SCO?			
8. Is the SSAA/SSP updated as follows:			
a. When hardware/software configuration changes occur?			
b. When the system is relocated?			
c. When the security mode/protection level changes?			
d. When connected to additional networks?			
9. Have all external connections to installed ISs been validated and approved by the DAA Rep/SCO?			
10. Are the ISSM/ISSOs aware of the SABI/TSABI process when connecting systems/networks of different classifications?			
SECTION C - IS & NETWORK SECURITY			
11. Are systems which process SCI information located in areas according to DCID 1-21?			
12. Is only authorized software being used?			
13. Are the ISSM, ISSOs/SAs, and users knowledgeable of virus protection and reporting procedures?			
14. Virus software			
a. Is the DoD-contract anti-virus software (Norton Anti-Virus or Network Associates VirusScan) running on all ISs? **[JDCSISSS 10.4.1]**			
b. Are the software version and signature files for each IS the most current available? **[DCID 6/3 5.B.1.a.4] & [JDCSISSS 10.4.1]**			
c. Is there a procedure in place for updating signature files on a monthly basis for all ISs including stand-alone systems? **[DCID 6/3 5.B.1.a.4]**			

d. Are procedures in place for dealing with virus incidents? **[JDCSISSS 8.3.3] [DCID 6/3 8.B.7]**			
e. Is anti-virus software setup to automatically run whenever media is introduced into the system? **[JDCSISSS 6.3.6]**			
15. Are documented software patches current and installation dates documented?			
a. Do all ISs use approved operating system software (Windows NT or Solaris)? **[Assistant Secretary of Defense Letter dated 22 Aug 96]**			
b. Are all game software removed from all ISs? **[JDCSISSS 11.6.3 11.6.4]**			
c. Is the Configuration Management (CM) plan current and is it being followed by all organizations within the Site/SCIF? **[DCID 6/3 2.B.7.c(7)]**			
d. Does the ISSM review all proposed hardware and software changes to the Site/SCIF? (Some minor changes may be made without ISSM approval such as switching out peripheral equipment and adding security patches to software programs) **[DCID 6/3 2.B.6.c(14)]**			
16. Audit Trails:			
a. Are audit trails enabled for every IS? **[JDCSISSS 7.5.3]**			
b. Are they set to capture the minimum events? **[JDCSISSS 7.5.3.1 and DCID 6/3 4.B.2.a.4.a, 4.B.2.a.4.d[1-3] and 4.B.2.a.5.a]**			
c. Are computers without automatic audit trails using ISSPM/SCO approved manual audit trails? [**JDCSISSS 7.5.3.2]**			
d. **Reviews being limited to the ISSM, or alternate, and ISSOs/SAs?**			
e. Are audit trails reviewed at least weekly or as directed by the ISSM and appropriate action taken, where applicable? **[JDCSISSS 7.5.3.4]**			
f. Summary reports and SCI system audits being maintained for five years? **[JDCSISSS 7.5.3.5] [DCID 6/3 4.B.2.a.4.c]**			
g. Are accounts audited at a minimum of annually to ensure old, unused accounts are deleted? **[JDCSISSS 7.5.1.4]**			
h. Are annual account audits documented? **[JDCSISSS 7.5.1.4]**			
17. Is the Access Request and Verification Roster:			
a. Acknowledged and signed?			
b. Periodically validated?			
c. Updated to indicate final access removal?			
d. Appropriately classified?			
e. Maintained by the SA?			
18. Account / Password Procedures			
a. Do all users have a unique login ID (or is a waiver on file from the DAA allowing group accounts)? **[JDCSISSS 6.3.1]**			

b. Is each password at least 8 alphanumeric/special characters long? **[JDCSISSS 6.3.2]**			
c. Do all ISs automatically invoke a password-protected screen lock after the IS is idle for more than 15 minutes? **[DCID 6/3 4.B.2.a.14.a and JDCSISSS 7.5.6]**			
d. Are users automatically logged out from ISs when they leave for an extended period of time? **[DCID 6/3 4.B.2.16.b and JDCSISSS 7.5.4]**			
e. Is the security clearance of each user verified to be equal to or greater than that of the IS to which they are gaining access prior to the issuance of the passwords.			
f. Is the need-to-know of each user verified prior to the issuance of the password? **[JDCSISSS 7.5.1.3]**			
g. Is each user or process granted the most restrictive set of privileges or access needed for the performance of authorized tasks? **[DCID 6/3 4.B.2.a.10]**			
h. Is the issuance of passwords documented with an NSA/CSS Form 6521 or similar form?			
i. Are initial passwords distributed in a secure manner? **[JDCSISSS 7.5.1.2]**			
j. Are passwords protected at the same level as the information they protect?			
k. Are passwords suppressed when entered?			
l. Are Access Authorization Letters retained for 1 year after access has been removed? **[JDCSISSS 7.5.1.2]**			
m. When users out-process the unit (for permanent departure), are they required to go through the ISSM (or designated individual) to have their active accounts terminated?			
n. When users out-process the unit for TDYs longer than 60 days, are they required to go through the ISSM (or designated individual) to have their active accounts disabled?			
o. Is the number of privileged users kept to a minimum? **[DCID 6/3 2.B.8.b(3)]**			
p. Are users with "group" privileges required to login as themselves prior to exercising their "group" privileges? (Users must not be able to login directly as "Root," "Administrator," or any other generic System group account) **[DCID 6/3 4.B.2.a.7.b]**			
q. Are there written procedures for establishing an account? (i.e. required paperwork and processes). **[DCID 6/3 4.B.2.a.3.b]**			
r. Are password "cracking" tools used to routinely check the strength of user passwords? **[DCID 6/3 4.B.2.a.9]**			
s. Is a history of old passwords (last 5recommended) kept by the system to prevent users from changing their password and then quickly changing back to their old password?			
t. Is there a minimum time that must expire before a user can change their password again? (90 days is recommended)			

u. Do all ISs limit the number of failed login attempts to no more than five (three is recommended)? **[DCID 6/3 4.B.2.a.16.c and JDCSISSS 7.5.5]**			
v. Are passwords changed quarterly for SBU and other classified systems, at least semiannually (180 days) for SCI systems?			
w. If a special situation warrants, are Group accounts approved by the DAA/SCO? **[JDCSISSS 7.5.1.6]**			
19. Are the ISSOs/SAs implementing the appropriate countermeasures to protect against vulnerabilities?			
20. Are procedures in effect to ensure the proper classification markings of all computer-generated products?			
21. Are appropriate Government warning banners and labels being used on systems?			
a. Are IS components (CPU, monitor, printer, scanner) marked with appropriate classification labels (e.g. 700-series or equivalent)? **[DCID 6/3 subsection 8.B.2 and JDCSISSS 6.3.7]**			
b. Is the Consent to Monitoring label attached to the monitor of all IS's. **[JDCSISSS 9.3.2]**			
c. Does a classification-warning banner appear on all systems that are using an approved KMM switch? **[JDCSISSS 1.5.10]**			
i. Are approved keyboard-monitor-mouse (KMM) switches installed between IS which are connected to a network or another IS at different classification levels?			
ii. Are appropriate procedures implemented and followed in using KMM switches?			
d. Has the proper authority approved the use of the KMM?			
e. Do all ISs display the approved Consent to Monitoring Banner prior to logging in?			
22. Is formal documentation used (i.e. 6522 or equivalent form) to record all IS release actions; are they completed and verified by appropriate IS personnel and filed with the SSAA/SSP?			
23. Are DD254s reviewed periodically to validate contractor access to data on SCI IS?			
24. Has an IS Contingency Plan:			
a. Been developed?			
b. Been successfully tested in the past year?			
c. Been periodically reviewed and updated?			
25. Does the approved SSAA/SSP and unit Standard Operating Procedures (SOPs) cover the following security related topics:			
a. Procedures for securely bringing the system up/down?			

b. Security responsibilities encompassing all personnel?			
c. Security marking of output products?			
d. Procedures for downgrading and/or releasing output or media?			
e. Procedures for media degaussing, destruction, and/or downgrading?			
f. Procedures for generating and reviewing the audit data?			
g. Procedures for adding/removing users from the IS/LAN?			
h. Procedures establishing access control privileges for users?			
i. Operational Security (OPSEC)?			
j. Virus and Incident reporting procedure?			
k. Contingency Plan procedures?			
l. Information Storage Media control and accounting procedures?			
m. Password Management procedures?			
n. Procedures for obtaining appropriate authorization to conduct monitoring of suspicious or illegal activity?			
26. Is the audit data protected by the Security Support Structure (operating system or security software)?			
27. Are data access controls automatically set to limit access when any new file or data set is created?			
28. Are system privileges limited to those necessary to perform assigned tasks (e.g. SUPERUSER, System Programmers, etc.)?			
29. Are the following features installed and activated?			
a. Screen Blanking			
b. Screen Lock			
c. Deadman Timeout			
30. If an IS (Fax) is connected to a STU-III/STE data port, has the appropriate approval letters been received from the proper authority? **[JDCSISSS 16.3.1.1]**			
a. Are written Operating Instructions been developed for Fax machine usage and located next to the machine? **[JDCSISSS 16.3.1.1.4]**			
b. Are audit log's used to record all transmissions over a Fax machine connected to a STU-III/STE? **[JDCSISSS 16.3.1.1.4]**			
31. Has the proper authority approved the use of the dial-in modems?			
32. Is the Auto Answering feature of all STU-IIIs/STEs configured IAW applicable policy?			
33. Has the proper authority approved the use of the STU-III/STE Auto Answering feature?			

Answering feature?			
34. Is the speaker phone feature disabled from all STU-IIIs within the SCIF (or is an appropriate waiver on file)? **[DCID 1/21 6.5.2]**			
35. Are unclassified ISs connected directly to the public telephone network; if so, has approval been received from proper authority?			
36. Is the use of dial-in modems connected to ISs/LANs IAW applicable policy?			
37. Are communications links connecting the components of the IS processing classified or sensitive unclassified information protected IAW National COMSEC policies?			
38. Are all critical systems backed up by an Un-interruptible Power Supply (UPS) system?			
39. Are IS microphones turned off or unplugged when not in use?			
40. Is the Red/Black separation criteria being strictly enforced?			
41. Has the operator and supervisor signed a PED acknowledgement form indication operating restrictions? **[JDCSISSS 15.4.1.1]**			
42. Has the SCIF Accreditation authority approved all PED for operation within the SCIF? **[JDCSISSS 15.4.1.1]**			
43. If PED's will be connected to a SCIF IS, has the ISSM given written approval on a case by case basis? **[JDCSISSS 15.4.1.2]**			
44. Has a case specific Standard Operating Procedure been developed for all PED's? **[JDCSISSS 15.4.2.1]**			
SECTION D - IS MAINTENANCE			
45. Has a maintenance policy and procedure been developed and implemented?			
46. Is a functional Configuration Management Program in place?			
47. Are personnel who perform maintenance on classified systems cleared and indoctrinated to the highest classification of information processed? **[JDCSISSS 13.3.1.1]**			
48. Are maintenance personnel U.S. citizens?			
49. Are uncleared maintenance personnel escorted by fully cleared and technically qualified personnel?			
50. Are IS components purged of all classified or unclassified information prior to removal from IS spaces, and are these actions appropriately documented?			
51. Are storage media removed from ISs prior to being released for service or repair?			

52. Are areas sanitized prior to maintenance performed by unclear personnel?			
53. Is a maintenance log, documenting repairs, used and maintained for the life of each IS? **[JDCSISSS 13.3.2.1]**			
54. Is a remote maintenance, diagnostic, and service transaction logs maintained for five years? **[JDCSISSS 13.3.4]**			
55. Are controls in place for maintenance of diagnostic hardware or software?			
SECTION E - INFORMATION STORAGE MEDIA CONTROL & LABELING			
56. Has a SOP been written outlining the procedures to be followed for the introduction and removal of storage media into and out of secure facilities IAW national policy?			
57. Has the Cdr/Commanding Officer publicized/developed policy identifying the level of control and accountability of information storage media in the organization?			
58. Have procedures been developed for the control of information storage media IAW national-level policy?			
59. Are media marked and labeled with the correct classification and handling instructions (Standard 700 series labels or equivalent, Privacy Act, Special Access Programs [SAP], etc.)?			
a. Are all diskettes labeled with the appropriate classification labels? **[JDCSISSS 12.4]**			
b. Are all diskettes labeled with SF711s (Data Descriptor Labels) and filled in with the organization, office symbol, and classification (of the data)? **[JDCSISSS 12.4.1]**			
c. Are all SF712 stickers supplemented with the highest level of associated caveats (Note: Do not use the SF Form 706 to supplement a TS marking) for the IS? (i.e. a label indicating "SI/TK/G" or the same thing written on the SF712 itself) **[DCID 6/3 subsection 8.B.2 and JDCSISSS 12.4.1]**			
d. Are CD-ROM cases, not the CD itself, labeled with the appropriate classification labels? **[JDCSISSS 12.4.1.1]**			
e. If required are CD-ROMs marked with a control number (using a non-toluene paint-pen) which matches a corresponding control number on its container or envelope (which is also labeled with the classification sticker)? **[JDCSISSS 12.4.1.1]**			
f. Are music CDs prohibited from all ISs? **[JDCSISSS 11.6.4]**			
60. Does the ISSM ensure excess or obsolete commercial software is free of classified information prior to release or reuse?			
61. Are procedures established which outline steps to be taken when transferring data to and from systems of unequal accreditation (classification and/or sensitivity)?			

62. Are reused removable media used at the same or higher classification level?			
63. Do users follow the approved procedures for transferring files from higher classified system to a lower classified system **[JDCSISSS 18.3.4]**			

APPENDIX A - REFERENCES

(U) The following publications are the primary security regulations associated with, and affecting Information Systems (IS) Intelligence operations. This appendix is not an inclusive list of all security regulations.

PUBLIC LAWS

Computer Fraud and Abuse Act, 18 U.S. Code section 1030, 1984.

Electronic Communications Privacy Act, 18 U.S. Code Section 2510, 1986.

Public Law 100-235, The Computer Security Act of 1987, 8 January 1988.

EXECUTIVE ORDERS

Executive Order 12333, United States Intelligence Activities, 4 December 1981.

Executive Order 12829, National Industrial Security Program, 6 January 1993.

Executive Order 12958, Classified National Security Information, 20 April 1995.

NATIONAL PUBLICATIONS

Common Criteria for Information Technology Security Evaluation, CCIB-98-026, Version 2.0, May 1998.

DCID 6/3, Director of Central Intelligence (DCI) Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems, 5 June 1999.

DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, Industry Annex, 12 April 2002.

DCID 6/1, Security Policy for Sensitive Compartmented Information and Security Policy Manual, 1 March 1995, Administrative Corrections 23 December 2002.

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs), 18 November 2002.

DCID 2/12P, Community Open Source Program, 1 March 1994.

The Intelligence Community Open Source Strategic Plan, 21 April 1993.

NSTISSAM TEMPEST/2-95, National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95 (formerly NACSIM 5203), Red/Black Installation Guidelines, 12 December 1995.

NSTISSI 3013, National Security Telecommunication and Information Systems Security Instruction (NSTISSI) 3013, Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal, 8 February 1990.

NSTISSI 4009, National Security Telecommunication and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary, September 2000.

NSTISSI 7000, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, TEMPEST Countermeasures For Facilities, 29 November 1993.

NSTISSI 7003, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 (C/NF), Protected Distribution Systems, 13 December 1996.

NSTISSP 11, National Information Assurance Acquisition Policy, dated January 2000.

NSTISSP 300, National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300, National Policy on Control of Compromising Emanations, 29 November 1993.

OMB Circular A-130, Management of Federal Information Resources, 15 July 1994, and principally, Appendix III, Security of Federal Automated Information, February 1996.

DEPARTMENT OF DEFENSE (DoD) PUBLICATIONS

DoD 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual (U), August 1998.

DoD Directive 5200.1-R, Information Security Program Regulation, January 1997.

DoD Directive 5200.2-R, Policy on Investigation and Clearance of DoD Personnel for Access to Classified Defense Information, 15 February 1986

DoD Directive C-5200.5, Communications Security (COMSEC), 21 April 1990.

DoD Directive C-5200.19, Control of Compromising Emanations, 16 May 1995.

DoD Directive 8500.1, Information Assurance, 24 October 2002..

DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.

DoD Directive 5220.22, DoD Industrial Security Program, 8 December 1980.

DoD 5220.22-R, Industrial Security Regulation, December 1985.

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995, and its Supplement, dated February 1995.

DoD Directive 5240.4, Reporting of Counterintelligence and Criminal Violations, 22 September 1992.

DEFENSE INTELLIGENCE AGENCY (DIA) PUBLICATIONS

DIA Manual 50-4, Department of Defense (DoD) Intelligence Information Systems (DoDIIS) Information Systems Security (INFOSEC) Program, 30 April 1997.

DIA Regulation 50-2, Information Security Program, 15 July 93.

Defense Intelligence Management Document SC-2610-141-93, DoDIIS Site Information Systems Security Officer's (ISSO) Handbook, November 1993.

Defense Intelligence Management Document DS-2610-142-00, DoD Intelligence Information System (DoDIIS) Security Certification and Accreditation Guide April 2000.

Defense Intelligence Management Document SC-2610-143-93, DoDIIS Site Certifier's Guide, November 1993.

NATIONAL SECURITY AGENCY (NSA)/CENTRAL SECURITY SERVICE (CSS) PUBLICATIONS

NSA/CSS Circular 25-5, Systems Acquisition Management, 3 April 1991.

NSA/CSS Circular 90-11, Protected Wireline Distribution System for COMINT Facilities, 7 June 1993.

NSA/CSS Classification Guide 75-98, 20 February 1998.

NSA/CSS Directive 21-1, DoD Computer Security Center Operations, 29 March 1984.

NSA/CSS Directive 130-1, Operational Information System & Network Security Policy, 13 March 1995.

NSA/CSS Manual 130-1, Operational Information Systems Security Manual, January 2001.

NSA/CSS Manual 130-2, Media Declassification and Destruction Manual, November 2000.

NSA/CSS Regulation 120-1, Reporting of Security Incidents and Criminal Violations, 16 March 1989.

NSA/CSS Regulation 120-24, STU-III Security Requirements, 25 April 2000.

NSA/CSS Regulation 130-2, Computer Virus Prevention Policy, March 1995.

NSA/CSS Regulation 130-3, Security Testing of NSA/CSS Automated Information Systems (IS) and Networks, 24 July 1992.

NSA/CSS Regulation 130-4, Connection of an Information System (IS) to the STU-III (type 1) Terminal Data Port, March 1995.

NSA/CSS Regulation 130-5, Use of Unclassified Publicly Accessible Computer Networks and information Systems such as the INTERNET (U), 15 July 1996.

USSID 12, United States Signals Intelligence (SIGINT) Directive 12, Automatic Data Processing (ADP) Policy for SIGINT Operations, 11 December 1990.

NSA/CSS Information Systems Certification and Accreditation Process (NISCAP), 31October 2002.

APPENDIX B – ACRONYMS & ABBREVIATIONS

(U) The following acronyms/abbreviations are expanded for clarification.

ACERT	Army Computer Emergency Response Team
AF	Air Force
AFCERT	Air Force Computer Emergency Response Team
AIA	Air Intelligence Agency
IS	Automated Information System
ASP	Accredited Security Parameters
ASSIST	Automated Systems Security Incident Support Team
AUTODIN	Automatic Digital Network
BDS	Broadband Distribution System
C&A	Certification and Accreditation
CCB	Configuration Control Board
CD	Compact Disk
CDE	Compact Disk Extra
CD-R	Compact Disk-Read
CDR	Critical Design Review
CD-ROM	Compact Disk-Read Only Memory
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CM	Configuration Management
CMB	Configuration Management Board
CO	Commanding Officer
COI	Community Of Interest
COMINT	Communications Intelligence
COMNAVSECGRU	Commander Naval Security Group
COMSEC	Communications Security
CONOP	Concept of Operation
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRYPTO	Cryptologic
CSE	Client-Server Environment
CSS	Central Security Service

CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving/Accrediting Authority
DAA Rep	Designated Approving/Accrediting Authority Representative (i.e., SCO)
DAC	Discretionary Access Control
DCI	Director, Central Intelligence
DCID	Director of Central Intelligence Directive
DEXA	DoDIIS Executive Agent
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DMS	Defense Messaging System
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information Systems
DOS	Disk Operating System
DRAM	Dynamic Random Access Memory
DSN	Defense Switching Network
DVD	Digital Video Disk
EEFI	Essential Elements of Friendly Information
EEPROM	Electronically Erasable Programmable Read Only Memory
EO	Executive Order
EPA	Environmental Protection Agency
EPROM	Erasable Programmable Read Only Memory
ERB	Engineering Review Board
FAX	Facsimile
FEPROM	Flash Erasable Programmable Read Only Memory
FOUO	For Official Use Only
FTS	Federal Telecommunications Service
FW&A	Fraud Waste & Abuse
GENSER	General Service
GOTS	Government Off-The-Shelf
HOIS	Hostile Intelligence Services
HQ	Headquarters
HSO	Host Security Office

IA	Information Assurance
IATO	Interim Approval To Operate
IATT	Interim Approval To Test
IAVA	Information Assurance Vulnerability Assessment
IAW	In Accordance With
IA	Information Assurance
ID	Identification
IG	Inspector General
INSCOM	Intelligence and Security Command
IOC	Initial Operational Capability
IR	Infrared
IS	Information System
ISD	Inspectable Space Determination
ISS	Information System Security
ISSE	Information Systems Security Engineer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSPM	Information Systems Security Program Manager
JAG	Judge Advocate General
LAN	Local Area Network
LOC	Level-of-Concern
LRU	Lowest Replaceable Unit
MILNET	Military Network
MO	Magneto-Optical
MOU	Memorandum Of Understanding
NACSIM	National COMSEC Information Memorandum
NAVCIRT	Navy Computer Incident Response Team
NCS	National Cryptologic School
NIMA	National Imagery and Mapping Agency
NIPRNET	uNclassified Internet Protocol Router NETwork
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISSIB	NSA/CSS Information System Security Incident Board
NOFORN	No Foreign National

NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSI	National Security Information
NSN	National Stock Number
NSO	Network Security Officer
NSTISSAM	National Security Telecommunications Information Systems Security Advisory Memorandum
NSTISSC	National Security Telecommunications Information System Security Committee
NSTISSI	National Security Telecommunications Information System Security Instruction
NSTISSP	National Security Telecommunications Information System Security Policy
Oe	Oersteds
OPSEC	Operational Security
PAA	Principal Accrediting Authority
PDA	Personal Digital Assistant
PDD	Personal Digital Diary
PDR	Preliminary Design Review
PDS	Protected Distribution System
PED	Portable Electronic Device
PL	Protection Level
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RF	Radio Frequency
RFI	Radio Frequency Interference
ROM	Read Only Memory
SA	System Administrator
SACS	Security Access Control System
SAP	Special Access Program
SAPI	Special Access Program - Intelligence
SBU	Sensitive But Unclassified
SCE	Service Cryptologic Element

SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	Service Certifying Organization (i.e., DAA Rep)
SDD	Secure Data Device
SDSO	System Design Security Officer
SF	Standard Form
SI	Special Intelligence
SIGAD	SIGINT Address
SIGINT	Signals Intelligence
SIM	System Integration Management
SIMO	System Integration Management Office
SIO	Senior Intelligence Officer
SISSPM	Senior Information Systems Security Program Manager
SOP	Standard Operating Procedure
SOW	Statement Of Work
SRAM	Static Random Access Memory
SSAA	System Security Authorization Agreement
SSAN	Social Security Account Number
SSO	Special Security Office/Special Security Officer
SSP	System Security Plan
STE	Secure Telephone Equipment
STU-III	Secure Telephone Unit III
ST&E	Security Test and Evaluation
T&E	Test and Evaluation
TDY	Temporary Duty
TK	Talent Keyhole
TS	Top Secret
UCMJ	Uniform Code of Military Justice
UPS	Un-interruptible Power Supply
US	United States
USERID	User Identification
USSID	United States Signals Intelligence Directive
USSS	United States SIGINT System
WAN	Wide Area Network

WORM Write Once Read Many

APPENDIX C – GLOSSARY OF TERMS

The following terms and definitions have been extracted from various documents and are provided for information and clarification. They are restricted to issues addressing information systems and related security matters.

Access. The ability and means to communicate with (input to or receive output from), or otherwise make use of any information, resource, or component in an information system (IS); or to have authorized entry to a specified area.

Accreditation. The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. This authorization is granted by the appropriate Designated Accrediting Authority (DAA), on a case-by-case basis, permitting the processing of SCI information on an IS. Approval is based upon the DAA's review of the SSAA/SSP. Under certain conditions interim approval-to-operate (IATO) may be granted by designees of the DAA.

Accredited Security Parameters (ASP). The security classification levels; compartments and subcompartments at which an information system (IS) or network is accredited to operate (e.g. Top Secret [TS]/Special Intelligence [SI]/Talent Keyhole [TK]).

Authentication. (1) To establish the validity of a claimed identity. (2) To provide protection against fraudulent transactions or logons by establishing the validity of a USERID, message, station, individual or originator.

Availability. Timely, reliable access to data and information services for authorized users.

Beta I. Security Certification testing performed in a lab environment or other facility as appropriate.

Beta II. Security Certification testing performed at designated operational installations(s) until stable baseline is achieved (configuration differences or other factors may necessitate multiple Beta II test sites).

BLACK. A designation applied to telecommunications and information systems (ISs), and to associated areas, circuits, components, and equipment, in which only unclassified signals are processed.

Broadband Distribution System (BDS). Any broadband system which can carry multiple channels of information. A BDS is not a local area network (LAN), however, it is capable of being the backbone for multiple LANs.

Buster. A computer program - part of the Computer Security Toolbox. BUSTER is a MS-DOS based program used to perform a binary search of a disk or diskette for any word or set of words found in a search definition file by performing a linear search on a disk or diskette, four sectors at a time. BUSTER uses the "LIMITS.TXT" file as its document for search word patterns.

Certification. The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certified TEMPEST Technical Authority (CTTA). A U.S. Government or U.S. Government contractor employee designated to review the TEMPEST countermeasures programs of a federal department or agency.

Classified Information. National security information (NSI) that has been classified pursuant to Executive Order 12958.

Clearing. Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Collateral. (1) Classified Non-Sensitive Compartmented Information (SCI) material to include General Service (GENSER) - an intelligence community term. (2) All national security information (NSI) classified under the provisions of an Executive Order (EO) for which special Intelligence community systems of compartmentation (i.e., SCI) are not formally established.

Command Authority. The individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Community-of-Interest (COI). A restricted network of users, each having an information system (IS) with an accredited security parameter identical to the others and having the need to communicate securely with other members of the network.

Compromising Emanations. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by telecommunications or information systems (IS) equipment. (See TEMPEST).

Computer Security (COMPUSEC). See INFOSEC.

Computer Security Toolbox. A set of tools designed specifically to assist Information Systems Security Officers (ISSOs)/System Administrators (SAs) in performing their duties. The functions within the TOOLBOX can erase appended data within files, eliminate appended data in free or unallocated space, search for specific words or sets of words for verifying classification and locating unapproved shareware programs. It also includes a program which allows you to clear laser toner cartridges and drums.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Control. The process of controlling modifications to a telecommunications or information system (IS) hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management. The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an information system (IS), throughout the development and operational life of the system.

Connectivity. A word which indicates the connection of two systems regardless of the method used in physical connection.

Contingency Plan. A plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with Disaster Plan and Emergency Plan.

Controlled interface. A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Critical Design Review (CDR). A formal review conducted on each configuration item when design is complete. Determines that the design satisfies requirements, establishes detailed compatibility, assesses risk, and reviews preliminary product specifications.

Crypto-Ignition Key (CIK). A device or electronic key used to unlock the secure mode of crypto equipment.

Cryptologic Information System (IS). A Cryptologic IS is defined as any IS which directly or indirectly supports the cryptologic effort, to include support functions, such as, administrative and logistics, regardless of manning, location, classification, or original funding citation. This includes strategic, tactical, and support ISs; terrestrial, airborne, afloat, in-garrison, and spaceborne ISs; ISs dedicated to information handling; and information-handling portions of ISs that perform other functions.

Declassification (of IS Storage Media). An administrative action following sanitization of the IS or the storage media that the owner of the IS or media takes when the classification is lowered to unclassified. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities. The procedures for declassifying media require Designated Accrediting Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) approval.

Defense Intelligence Agency (DIA). The Director, DIA is the authority for the promulgation of intelligence information systems (ISs) computer security policy, and is also the Principal Approving Authority (PAA) for the Security Accreditation against that policy of all ISs and networks processing, using, storing, or producing intelligence information.

Degauss. (1) To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force commonly referred to as demagnetizing, or (2) to reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data. NOTE: A list of approved degaussers is updated and published quarterly in the “National Security Agency (NSA) Information Security Products and Services Catalog”.

Department/Agency/Organization (DAO) Code. A 6-digit identification number assigned by the Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) Central Facility to organizational descriptions. The DAO code must be used by units when placing an order for STU-III/STE keying material.

Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system (or network) at an acceptable level of risk.

DAA Representative (DAA Rep). An official or service certification organization (SCO) responsible for ensuring conformance to prescribed security requirements for components of sites under their purview. SCOs are listed in the Department of Defense Intelligence Information Systems (DoDIIS) Information System Security Officer (ISSO) Handbook.

Destroying. Destroying is the process of physically damaging the media to the level that the media is not usable, and that there is no known method of retrieving the data.

Discretionary Access Control (DAC). A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Diskette. A metal or plastic disk, coated with iron oxide, on which data are stored for use by an information system (IS). The disk is circular, rotates inside a square lubricated envelope that allows the read/write head access to the disk.

Department Of Defense (DoD) Intelligence Information Systems (DoDIIS). The aggregation of DoD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence to military commanders and national level decision makers. For the purpose of this document, DoDIIS encompasses the Military Services, Defense Agencies, Defense Activities, Offices of the Secretary and Assistant Secretaries of Defense, the Organization of the Joint Chiefs of Staff, and the Unified Commands.

DoDIIS Site. An administrative grouping of a combination of Department of Defense Intelligence Information Systems (DoDIIS) accredited and managed collectively on the basis of geographical or organizational boundaries. Each DoDIIS Site contains multiple DoD intelligence information systems (ISs) which support the site's intelligence mission.

EEPROM. Acronym for electrically erasable programmable read-only memory. Pronounced double-e-prom or e-e-prom, an EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge. Like other types of PROM, EEPROM retains its contents even when the power is turned off. Also like other types of ROM, EEPROM is not as fast as RAM. EEPROM is similar to flash memory (sometimes called flash EEPROM). The principal difference is that EEPROM requires data to be written or erased one byte at a time whereas flash memory allows data to be written or erased in blocks. This makes flash memory faster.

EPROM. Acronym for erasable programmable read-only memory, and pronounced e-prom, EPROM is a special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents, making it possible to reprogram the memory. To write to and erase an EPROM, you need a special device called a PROM programmer or PROM burner. An EPROM differs from a PROM in that a PROM can be written to only once and cannot be erased. EPROMs are used widely in personal computers because they enable the manufacturer to change the contents of the PROM before the computer is actually shipped. This means that bugs can be removed and new versions installed shortly before delivery. A note on EPROM technology: The bits of an EPROM are programmed by injecting electrons with an elevated voltage into the floating gate of a field-effect transistor where a 0 bit is desired. The electrons trapped there cause that transistor to conduct, reading as 0. To erase the EPROM, the trapped electrons are given enough energy to escape the floating gate by bombarding the chip with ultraviolet radiation through the quartz window. To prevent slow erasure over a period of years from sunlight and fluorescent lights, this quartz window is covered with an opaque label in normal use.

Fixed Disk. A magnetic storage device used for high volume data storage and retrieval purposes, which is not removable from the disk drive in which it operates.

Flash Memory. A special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can easily be updated if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.

Flush. A computer program which is part of the Computer Security Toolbox. FLUSH is a MS-DOS based program used to eliminate appended data within a file or files and appended data located in unallocated or free space on a disk or diskette.

FRAM. Short for Ferro electric Random Access Memory, a type of non-volatile memory developed by Ramtron International Corporation. FRAM combines the access speed of DRAM and SRAM with the non-

volatility of ROM. Because of its high speed, it is replacing EEPROM in many devices. The term FRAM itself is a trademark of Ramtron.

General User. A person accessing an information system (IS) by direct connections (e.g., via terminals) or indirect connections. NOTE: "Indirect connection" relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

Government-Approved Facility. Any Government owned room or outside of a Sensitive Compartmented Information Facility (SCIF) with controlled or restricted access designed to limit public access which has operational procedures in place to actually limit access; any Government owned SCIF or area within a SCIF.

Guest system. Any system that enters the SCIF which has not already been certified or accredited by the respective cognizant SCIF authority is considered a Guest system.

Hard Disk. A magnetic storage device used for high volume data storage and retrieval purposes to include ones which are both removable and non-removable from the disk drives in which they operate.

Information Assurance. Information Operations that protect and defend data and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing restoration of IS by incorporating protection, detection, and reaction capabilities.

Information System (IS). Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data (digital or analog) and includes software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Information Systems (IS) and Network Security. IS and network security is the protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and the information contained within the system. Such protection is the integrated application of communications security (COMSEC), TEMPEST, and information systems security (INFOSEC) executed in liISon with personnel security, operations security, industrial security, resources protection, and physical security.

Information Systems Security (INFOSEC). The protection of information systems (ISs) against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information Systems Security Engineer (ISSE). The person responsible for ensuring the security and integrity of a system during its life cycle and interfacing with other program elements to ensure security functions and safeguards are effectively integrated into the total system engineering effort. See SDSO.

Information Systems Security Manager (ISSM). The manager responsible for an organization's IS security program. Appointed by the Commander/Commanding Officer, the ISSM is the single point of contact for his/her organization concerning security matters to the Designated Accrediting Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO).

Information Systems Security Program Manager (ISSPM). The Air Force (AF) Air Intelligence Agency (AIA)/Army Intelligence and Security Command (INSCOM)/Navy Commander, Naval Security Group (COMNAVSECGRU) individual appointed by the Service Cryptologic Element (SCE) Commander/Commanding Officer as being the manager responsible for the SCE-level information systems (IS) and network security program and the security of all the agency's/command's ISs. Additionally, the

ISSPM is the Designated Accrediting Authority (DAA) for the accreditation of systems on behalf of the NSA/CSS Senior Information Systems Security Program Manager (SISSPM).

Information Systems Security Officer (ISSO). The person responsible to the ISSM for ensuring that operational security is maintained for a specific IS, sometimes referred to as a Network Security Officer. Each organizational level unit assigns one ISSO per system. A ISSO may have the responsibility for more than one system. See System Administrator (SA).

Inspectable Space. A determination of the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

Integrity. Protection against unauthorized modification or destruction of information. Evident as an IS Security characteristic ensuring computer resources operate correctly and data in the system is accurate. This characteristic is applicable to hardware, software, firmware, and the databases used by the computer system.

Intelligence Community. A term which, in the aggregate, refers to the following Executive Branch organizations and activities: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); offices within the Department of Defense; and others organized for collection of specialized national foreign intelligence through reconnISsance programs.

Interconnected System. A set of separately accredited systems that are connected together.

Interim Approval To Operate (IATO). Temporary authorization granted by a Designated Accrediting Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) for an information system (IS) to process classified information in its operational environment based on preliminary results of a security evaluation of the system.

Interoperability. The capability of one system to communicate with another system through common protocols.

Initial Operating Capability (IOC). A time when the persons in authority (e.g. program/project managers [PMs] or operations personnel) declare that a system meets enough requirements to formally be declared operational while the system may not meet all of the original design specifications to be declared fully operational.

Key Material Identification Number (KMID). A unique number automatically assigned to each piece of Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) keying material by the STU-III/STE.

Laptop. See Portable Computer System.

Level of Concern. The Level of Concern is a rating assigned to an IS by the DAA. A separate Level of Concern is assigned to each IS for confidentiality, integrity and availability. The Level of Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level of Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes and transmits. The Level of Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level of Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed, and transmitted by the systems for mission accomplishment, and how much tolerance for delay is allowed.

Limited Release. A procedure to be used by United States SIGINT System (USSS) activities to control the release of storage media devices that have contained classified information to other activities outside the USSS community.

Local Area Network (LAN). Any local area capability to provide interoperability. See network.

Logic Bomb. A logic bomb is a program or code fragment which triggers an unauthorized, malicious act when some predefined condition occurs. The most common type is the "time bomb", which is programmed to trigger an unauthorized or damaging act long after the bomb is "set". For example, a logic bomb may check the system date each day until it encounters the specified trigger date and then executes code that carries out its hidden mission. Because of the built-in delay, a logic bomb virus is particularly dangerous because it can infect numerous generations of backup copies of data and software before its existence is discovered.

Malicious Code. Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an IS. It may be included in hardware, software, firmware or data. Computer Viruses, Worms, Trojan Horses, Trapdoors, and Logic/Time Bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to ISs because of their reproductive capability.

Malicious Code Screening. Screening is the process of monitoring for the presence of malicious code. Malicious code occurs in different forms, which may have different methods for screening. Malicious code can arrive through either media that are introduced to IS or as mobile code that arrives through connections to other systems and networks.

Master Crypto-Ignition Key (CIK) Custodian. An individual at each node in a Community of Interest (COI) who is responsible for controlling and maintaining the Master CIK and programming the security features of the Secure Telephone Unit (STU)-III/STE.

Mission-Essential. In the context of information, that information which is an essential portion of a unit's mandatory wartime capability.

Mobile Code. The code obtained from remote systems, transmitted across a network, and then downloaded onto and executed on a local system. Mobile code has come to refer to web-based code downloaded onto a user's client and run by the user's browser. The larger set of mobile code normally involves an explicit decision to execute—either by the user (manually) or by an application—and an implicit decision autonomously made by an application.

Modem. A device that electronically Modulates and Demodulates signals, hence the abbreviation MODEM.

National Security Agency/Central Security Service (NSA/CSS). The Director, NSA/CSS is the authority for promulgation of computer security policy, and is also the Principal Approving Authority (PAA) for the security accreditation against that policy of all information systems (ISs) and networks processing, using, storing, or producing cryptologic information.

National Security Information (NSI). Information that has been determined, pursuant to Executive Order (EO) 12958 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

National Security-Related Information. Unclassified information related to national defense or foreign relations of the United States.

Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient of information requires access to specific classified information to perform or assist in a lawful and authorized Government function, such as that required to carry out official duties.

Network. A combination of information transfer resources devoted to the interconnection of two or more distinct devices, systems, or gateways.

Network Manager. The individual who has supervisory or management responsibility for an organization, activity, or functional area that owns or operates a network.

Network Security Officer (NSO). An Individual formally appointed by a Designated Accrediting Authority (DAA)/Service Certifying Organization (SCO) to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an information system (IS) network.

Network System. A system that is implemented with a collection of interconnected network components. A network system is based on a coherent security architecture and design.

Non-Volatile Memory Components. Memory components that DO RETAIN data when all power sources are disconnected.

Notebook. See Portable Computer System.

NVRAM. Abbreviation of Non-Volatile Random Access Memory, a type of memory that retains its contents when power is turned off. One type of NVRAM is SRAM that is made non-volatile by connecting it to a constant power source such as a battery. Another type of NVRAM uses EEPROM chips to save its contents when power is turned off. In this case, NVRAM is composed of a combination of SRAM and EEPROM chips.

Object Reuse. Reassignment of a storage medium (e.g., page frame, disk sector, or magnetic tape) that contained one or more objects, after ensuring that no residual data remained on the storage medium.

Optical Storage Media. Optical mass storage, including compact disks (CD, CDE, CDR, CDROM), optical disks (DVD), and magneto-optical disks (MO)

Orange Book. Synonymous with the Department of Defense (DoD) Trusted Computer System Evaluation Criteria, DoD 5200.28-STD.

Organizational-level Commander/Commanding Officer. The individual, regardless of rank, which has been appointed as the officer-in-command of a physical organization.

Overwrite Procedure (for purposes of downgrading in limited cases). Process which removes or destroys data recorded on an information system (IS) storage medium by writing patterns of data over, or on top of, the data stored on the medium.

Overwrite Verification Procedure. A visual validation procedure that provides for reviewing, displaying, or sampling the level of success of an overwrite procedure.

Palmtop. See Portable Computer System.

Pass Phrase. Sequence of characters, longer than the acceptable length of a password that is transformed by a password system into a virtual password of acceptable length.

Password. Protected/private character string used to authenticate an identity or to authorize access to data.

Password Shadowing. The ability within any operating system which physically stores the password and/or encrypted password results in a mass storage area of the system other than the actual password file itself. This feature prevents the theft of passwords by hackers. Usually a UNIX feature.

Periods Processing. The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be cleared of all information from one processing period before transitioning to the next. A system is said to operate in a “Periods Processing” environment if the system is appropriately sanitized between operations in differing protection level periods, or with differing user communities or data.

Peripheral. Any devices which are part of an information system (IS), such as printers, hard and floppy disk drives, and video display terminals.

Personal Digital Assistants (PDA)/Diaries (PDD). These items are mini processors with computing power that are generally smaller than laptop, notebook, or palmtop computers. Some examples include, but are not limited to, the Newton, Boss, Wizard, etc.

Phonemes. A phonetic word which sounds similar to an actual word. (Example, "fone" for "phone," "lafter" for "laughter").

Portable Computer System. Any computer system specifically designed for portability and to be hand carried by an individual (e.g., Grid, Laptop, Notebook, Palmtop, etc.).

Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for all IS within an agency. Within the intelligence community, the PAAs are the DCI, EXDIR/CIA, AS/DOS (Intelligence and research), DIRNSA, DIRDIA, ADIC/FBI (National Security Div.), D/Office of Intelligence/DOE, SAS/Treasury (National Security), D/NIMA and the D/NRO.

Privacy (Not Security). The rights of an individual or organizations to determine for themselves when, how, and to what extent information about them is to transmitted to others.

Privileged User. The user of an information system (IS) who has root user authority.

Project/Program Manager (PM). The single individual responsible for a project or program who manages all day-to-day aspects of the project or program.

PROM. Pronounced prom, an acronym for programmable read-only memory. A PROM is a memory chip on which data can be written only once. Once a program has been written onto a PROM, it remains there forever. Unlike RAM, PROMs retain their contents when the computer is turned off. The difference between a PROM and a ROM (read-only memory) is that a PROM is manufactured as blank memory, whereas a ROM is programmed during the manufacturing process. To write data onto a PROM chip, you need a special device called a PROM programmer or PROM burner. The process of programming a PROM is sometimes called burning the PROM. An EPROM (erasable programmable read-only memory) is a special type of PROM that can be erased by exposing it to ultraviolet light. Once it is erased, it can be reprogrammed. An EEPROM is similar to a PROM, but requires only electricity to be erased.

Protected Distribution System (PDS). A wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Protocols. Set of rules and formats, semantic and syntactic, that permits entities to exchange information.

Public Domain Software. Programs/software that is uncopyrighted because the author intended to share them with everyone in the public domain. Source code is usually included and the author grants you the right to copy, distribute and modify the software.

Purge. The removal of data from an information system (IS), its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. Note: An IS must be disconnected from any external network before a purge. See Clearing.

RED. A designation applied to telecommunications and information systems (ISs), plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

Red/Black Concept. Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Remote Maintenance. An operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system), remote service for analysis or maintenance.

Removable Hard Disk. A hard disk contained in a removable cartridge type casing.

Risk Analysis. Synonymous with Risk Assessment.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an information system (IS), and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management. The discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level.

Routine Changes. Changes which have a minimal effect on the overall TEMPEST security of the Sensitive Compartmented Information (SCI) Facility (SCIF). Adding a different type of electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment within the facility, and minor installation changes are examples of routine changes.

Sanitizing (Also Purging). The removal of information from media or equipment such that the data recovery using any known technique or analysis is prevented, as well as the removal of all classified labels and markings. Sanitizing allows moving the media to an environment with lower protection requirements. In general, laboratory techniques cannot retrieve data that has been sanitized/purged.

Sealed Disk Drive. See “Hard Disk”.

Secure Copy. A computer program which is part of the Computer Security Toolbox. Secure Copy (SCOPY) is a MS-DOS based program used to eliminate appended data within a file or files while transferring the same from a source disk or diskette to a target disk or diskette.

Secure Data Device (SDD). The SDD provides a simple and cost-effective way to protect classified Government data transmissions. The SDD provides Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) secure data transmission functions without voice features and is fully interoperable with all other STU-III/STE products. It allows the user to access a computer database, send a facsimile (FAX) message, or use electronic mail and be sure the information is protected. The SDD was developed under the U.S. Government’s STU-III/STE program and is approved for use by Federal departments, agencies, and Government contractors.

Secure Telephone Unit III (STU-III). The STU-III family includes several interoperable terminals capable of transmitting voice and data through the public telephone network. The STU-III can be used as an ordinary telephone, and can also be used as a secure terminal, connected through the public telephone network to other STU-IIIs. A STU-III Secure Data Device (SDD) provides STU-III secure data transmission functions without voice features. STU-IIIs are endorsed by the National Security Agency (NSA) for protecting classified or sensitive, unclassified U.S. Government information, when appropriately keyed.

Security. The protection of information to assure it is not accidentally or intentionally disclosed to unauthorized personnel.

Security Environment Changes. Changes which have a detrimental effect on the facility. Changes to the inspectable space (IS), addition of a radio transmitter or a modem for external communications, removal or reduction of an existing TEMPEST countermeasure (Radio Frequency Interference [RFI] Shielding, Filters, Control/Inspectable space, etc.) would be changes to the security environment.

Security Testing. The process to determine that an information system (IS) protects data and maintains functionality as intended.

Security Training, Education and Motivation (STEM). A security education program designed to educate and motivate personnel concerning the protection of priority resources and the safeguarding of classified information.

Senior Information Systems Security Program Manager (SISSPM). The national-level individual appointed by the Director, National Security Agency (DIRNSA) as being the manager responsible for the national-level Service Cryptologic Element (SCE) Information Systems (IS) and Network Security Program, the security of all Cryptologic ISs, and is the Designated Accrediting Authority (DAA) for the accreditation of systems on behalf of the DIRNSA.

Senior Intelligence Officer (SIO). The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, or element of an intelligence community organization or Department of Defense (DoD) Intelligence Activity assigned responsibilities or designated authorities by a Senior Official of the Intelligence Community (SOIC).

Senior Officials of the Intelligence Community (SOIC). The heads of organizations or their designated representatives within the Intelligence Community, as defined by Executive Order (EO) 12333.

Sensitive But Unclassified (SBU) Information. Information collected, maintained, and/or disseminated by an agency that is not classified but whose unauthorized release or use could compromise or damage privacy or proprietary rights, critical agency decision making, and/or the enforcement or implementation of public law or regulations under which the agency operates.

Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19).

Sensitive Compartmented Information (SCI) Facility (SCIF). An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed and/or electronically processed.

Service Certifying Organization (SCO). The organization responsible for ensuring conformance to prescribed security requirements for components of sites under their purview. SCOs are listed in the Department of Defense Intelligence Information Systems (DoDIIS) Information System Security Officer (ISSO) Handbook.

Service Cryptologic Elements (SCE). A term used to designate, separately or together, those elements of the U.S. Army, Navy, and Air Force which perform cryptologic functions. The Air Force Air Intelligence Agency (AIA), Army Intelligence and Security Command (INSCOM), and Navy Commander Naval Security Group (COMNAVSECGRU) are the SCEs responsible to the National Security Agency/Central Security Service (NSA/CSS) for accreditation of all cryptologic information systems (ISs) within their respective services.

Site Information Systems Security Manager (Site ISSM). The single information systems (IS) security focal point for a defined site. The site ISSM supports two organizations: User organization and technical

organization. The site ISSM is responsible for managing the baseline and ensuring that changes to the site baseline are properly controlled.

Site Integration Management Office (SIMO). The major functions of the SIMO are: Establishing baselines, monitoring compliance, configuration management, and integration transition. There are three levels of such offices: DoDIIS, Service, and site. Only the larger sites will have a site SIMO.

Special Access Program (SAP). Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine "need-to-know"; or special lists of persons determined to have a "need-to-know".

Special Security Officer (SSO). The individual assigned responsibility for the security management, operation, implementation, use and dissemination of all Sensitive Compartmented Information (SCI) material within his/her respective organization.

Stand-Alone System. An information system (IS) operating independent of any other IS within an environment physically secured commensurate with the highest classification of material processed or stored thereon.

Survivability. The capability of a system to withstand a man-made or natural hostile environment without suffering an abortive impairment of its ability to accomplish its dedicated mission.

SYSOP. An operator responsible for performing system-oriented procedures. See System Administrator.

System. A generic name for an Information System (IS).

System Administrator (SA). The individual responsible for maintaining the system in day-to-day operations. The SA has responsibility to: manage system hardware and software, data storage devices and application software; manage system performance; provide system security and customer support; perform equipment custodian duties; maintain software licenses and documentation; monitor hardware and software maintenance contracts; establish USERIDs and passwords; ensure adequate network connectivity; review audit trails; and provide backup of system operations and other system unique requirements. See Information System Security Officer (ISSO).

System Design Security Officer (SDSO). An individual responsible for ensuring that adequate security requirements are stated in the design specifications of new systems and system upgrades during the design phase of their life cycle. This individual works closely with all project/program acquisition managers. See ISSE.

System Security Engineering. The efforts that help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort.

System Security Authorization Agreement (SSAA). A formal document that fully describes the planned security tasks required to meet system or network security requirements. The package must contain all information necessary to allow the DAA Rep/SCO to make an official management determination for authorization for a system, network, or site to operate in a particular security mode of operation; with a prescribed set of safeguards, against a defined threat with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to external systems; and at an acceptable level of risk.

System Security Plan (SSP). See System Security Authorization Agreement.

Technical Vulnerability. A hardware, firmware, communication, or software weakness which leaves an information system (IS) open for potential exploitation or damage, either externally or internally resulting in risk for the owner, user, or manager of the IS.

TEMPEST. A short name referring to investigation, study, and control of compromising emanations from telecommunications and information system (IS) equipment. TEMPEST must be considered during all life cycle phases of equipment. (See Compromising Emanations).

TEMPEST Approved. This term applies to equipment or systems which have been built and certified to meet Level I of National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements.

TEMPEST Zone. A defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated without emanating electromagnetic radiation beyond the controlled space boundary of the facility.

TEMPEST Zoned Equipment. Equipment that has been evaluated and assigned an equipment zone corresponding to the level in National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92. This equipment must be installed according to the NSTISSAM and HQ-Level specialized installation instructions.

Terminal Area. A subset or part of the overall work space assigned to a specific area within an organization. An area within the typical office environment restrictive in size such that it permits one person to observe and monitor access with the intent of preventing Information System (IS) abuse and unauthorized IS access.

Threat Assessment. The process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Threat Monitoring. The analysis, assessment, and review of Information Systems (ISs) audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security.

Toolbox. See Computer Security Toolbox.

Trapdoor. Operating system and application safeguards that usually prevent unauthorized personnel from accessing or modifying programs. During software development, however, these built-in security measures are usually bypassed. Programmers often create entry points into a program for debugging and/or insertion of new code at a later date. These entry points (trapdoors) are usually eliminated in the final stages of program development, but they are sometimes overlooked, accidentally or intentionally. A perfect example of a trapdoor was dramatized in the movie War Games, where the teen-age hacker enters the special password “Joshua” and gains unrestricted access to a mainframe computer in NORAD headquarters. Such a mechanism in a computer’s operating system can grant an attacker unlimited and virtually undetectable access to any system resource after presenting a relatively trivial control sequence or password.

Trojan Horse. A computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification, or destruction of data. This is the most commonly used method for program-based frauds and sabotage.

Trusted Computing Base (TCB). The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. NOTE: The ability of a TCB to enforce correctly a unified security policy depends on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Trusted Path. A mechanism by which a person using a terminal can communicate directly with the trusted computing base (TCB). **NOTE:** The trusted path can only be activated by the person or the TCB and cannot be initiated by untrusted software.

uNclassified Internet Protocol Router NETwork. The unclassified network which replaced the military unclassified network. Provides connection to the world wide web.

Unclassified Sensitive. For computer applications, this term refers to any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under the criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987, Public Law 100-235). Also see Sensitive but Unclassified (SBU) Information.

User Identification (USERID). A unique symbol or character string that is used by an information system (IS) to uniquely identify a specific user.

User Network Manager (UNM). Each sponsor of a Community-of-Interest (COI) must designate an individual who will be responsible for the management of the network, request permission to use the data port, and ensure compliance with the security procedures defined in appropriate security policy documents and those specifically defined in the approval process.

User Representative (UR). A person formally designated, on behalf of the Command Authority, who is responsible for preparing and submitting all key orders (including Sensitive Compartmented Information [SCI]) to the Central Facility. The UR has the responsibility for monitoring the status of those orders, to include keeping the Communications Security (COMSEC) manager informed of the pending key request in situations where the UR is other than the COMSEC manager.

Virus. A self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Volatile Memory. Random Access Memory (RAM) which is not retained upon system shutdown.

Vulnerability. A weakness in an information system (IS), or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls), that could be exploited.

Wide Area Network (WAN). A computer network that services a large area. WANs typically span large areas (states, countries, and continents) and are owned by multiple organizations. See Local Area Network and Network.

Worm. A worm is a program, originally developed by systems programmers, which allows the user to tap unused network resources to run large computer programs. The worm would search the network for idle computing resources and use them to execute a program in small segments. Built-in mechanisms would be responsible for maintaining the worm, finding free machines, and replicating the program. Worms can tie up all the computing resources on a network and essentially shut it down. A worm is normally activated every time the system is booted up. This is differentiated from WORM (write-once, read many) descriptive of optical (compact disk) media with single write capability.

Write Protect. A term used to indicate that there is a machine hardware capability which may be manually used to protect some storage media from accidental or unintentional overwrite by inhibiting the write capability of the system. (For example, write protection of magnetic tapes is accomplished by the physical removal of the “write-ring” from the back of the tape. Write protection of three and one half inch floppy diskettes refers to the correct placement of the sliding tab to the open position which inhibits the hardware

capability to perform a physical write to the diskette. Write protection includes using optical disks within CD read-only devices.)

APPENDIX D - SUMMARY OF CHANGES