

DEPARTMENT OF THE ARMY UNITED STATES ARMY INFORMATION SYSTEMS ENGINEERING COMMAND FORT HUACHUCA, ARIZONA 85613-5300



SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) TECHNICAL IMPLEMENTATION CRITERIA

VERSION 6

OCTOBER 2010

FORT DETRICK ENGINEERING DIRECTORATE

Distribution C

Distribution authorized to U.S. Government agencies and their contractors only, for administrative or operational use, as of October 2010. Refer other requests for this document to Director, U.S. Army Information Systems Engineering Command, Fort Detrick Engineering Directorate, ATTN: ELIE-ISE-DE, Fort Detrick, MD 21702-5047.



DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for advertisement.

CHANGES

Refer requests for all changes that affect this document to: USAISEC, ATTN: ELIE-ISE-DE, Fort Detrick, MD 21702-5047.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements. SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) TECHNICAL IMPLEMENTATION CRITERIA

VERSION 6

OCTOBER 2010

U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND FORT DETRICK ENGINEERING DIRECTORATE

Distribution C

Distribution authorized to U.S. Government agencies and their contractors only, for administrative or operational use, as of October 2010. Refer other requests for this document to Director, U.S. Army Information Systems Engineering Command, Fort Detrick Engineering Directorate, ATTN: ELIE-ISE-DE, Fort Detrick, MD 21702-5047.

KIMBERLY K. REED Group Leader, Data Team Fort Detrick Engineering Directorate

EUGENE W. BAKER Director Fort Detrick Engineering

ALBERT M. RIVERA Technical Director U.S. Army Information Systems Engineering Command

TABLE OF CONTENTS

	Page
1.0 INTRODUCTION	1
1.1 Purpose	1
1.2 Scope	1
1.3 SIPRNET Project Goal	1
1.4 Disclaimer	2
1.5 Mandatory and Advisory Terminology	2
2.0 REFERENCES	2
2.1 National Security Agency (NSA) Publications	2
2.2 Department of Defense (DOD) Publications	4
2.3 Defense Information Systems Agency (DISA) Publications	5
2.4 Department of the Army (DA) Publications	5
2.5 Miscellaneous Publications	6
3.0 MAJOR PARTICIPANTS AND RESPONSIBILITIES	8
3.1 U.S. Army Information Systems Engineering Command (USAISEC)	8
3.2 Designated Approving Authority (DAA)	8
3.2 NEC / Communications Provider	8
3.4 Local Site / User / Tenant IMO	9
3.5 Army CTTA	10
3.6 Joint	10
4.0 TECHNICAL SOLUTIONS DESCRIPTION AND CRITERIA	10
4.1 SIPRNET Programs	10
4.2 Connectivity Areas of Responsibility	12
4.3 Access Areas and Threat Levels	17
4.4 Protected Distribution Systems (PDS)	20
4.5 SIPRNET Physical Architecture	25
4.6 Tunneling	31
4.7 Installation of PDS	31
4.8 Encryption Devices	39
4.9 Secure wireless Local Area Networks (SwLANS)	45
4.10 Voice over Secure Internet Protocol (VOSIP)	40
4.11 Video Teleconterenting (VTC)	52
4.12 Information Assurance (IA)	50
5.0 SIPRNET CONNECTION PROCESS	57
5.1 DISN Connection Approval Process (CAP)	61
5.2 Accreditation and ATC	62
6.0 COST MODELING AND ESTIMATING FOR FINANCIAL PLANNING	64
61 General	64
6.2 Cost Typing	65
6.3 Funding Requirements and Limitations	66

Page

Appendices

Appendix A. Figures, Drawings, and Diagrams	A-1
Appendix B. Encryption Devices	B-1
Appendix C. PDS Inspection Checklist	C-1
Appendix D. Sample SIPRNET Site Survey Considerations	D-1
Appendix E. SIPRNET User and Allocation Tables	E-1
Appendix F. SIPRNET Allocations for New Military Construction	F-1
Appendix G. Sample SOP for SIPRNET Connections	G-1
Appendix H. Sample SIPRNET PDS Specification for BRAC/MCA Construction	H-1
Appendix I. SIPRNET Gross Cost Estimation Tool	I-1
Appendix J. Sample IPS Containers with Movable Racks	J-1
Appendix K. MCA/BCA Funding Breakout	K-1
Glossary. Abbreviations, Acronyms, And DefinitionsGl	lossary-1

Tables

Table 1. VoSIP Area Codes	51
Table B-1. COMSEC Device NSNs	B-1
Table E-1. User Allocation and Distribution at Brigade HQ BCT	E-1
Table E-2. User Allocation and Distribution at Battalion BCT	E-2
Table E-3. User Allocation and Distribution at Division HQ	E-3
Table E-4. User Allocation and Distribution at Corps HQ	E-4
Table E-5. User Allocation and Distribution at School Commandant and U.S. Army	
Engineer School	E-5
Table E-6. User Allocation and Distribution at Depot Commander and Production	
Operations	E-5
Table E-7. User Allocation and Distribution at Garrison Commander and Garrison	
Directorates	E-6
Table F-1. SIPRNET for New Military Construction	F-1

Figures

Figure A-1.	Example of WAN, MAN, CAN, and LAN	A-2
Figure A-2.	SIPRNET High-Level Overview	A-3
Figure A-3.	DISA-Managed SIPRNET Assets	A-4
Figure A-4.	NEC-Managed SIPRNET Assets	A-5
Figure A-5.	Tenant-Managed SIPRNET Assets	A-6
Figure A-6.	SIPRNET Dial-Up Example	A-7
Figure A-7.	PDS Physical Architecture Example	A-8
Figure A-8.	Wireless Architectures	A-9
Figure A-9.	Secure-Only ISDN or IP VTC	. A-10
Figure A-10	. Multi-Domain ISDN or IP VTC	. A-10
Figure A-5. Figure A-6. Figure A-7. Figure A-8. Figure A-9. Figure A-10	Tenant-Managed SIPRNET Assets SIPRNET Dial-Up Example PDS Physical Architecture Example Wireless Architectures Secure-Only ISDN or IP VTC Multi-Domain ISDN or IP VTC	A-6 A-7 A-8 A-9 . A-10 . A-10

PageFigure B-1. Evolution of INEs.B-2Figure B-2. Evolution of LEF.B-12Figure B-3. Evolution of Key ManagementB-15Figure J-1. Hamilton IPS Clearance RequirementsJ-2Figure J-2. Hamilton IPS DimensionsJ-3Figure J-3. Trusted Systems IPS Clearance RequirementsJ-4Figure J-4. Trusted Systems IPS DimensionsJ-5

Attachments

Attachment 1.	Draft Memorandum, Army CTTA, Subject: Updated Installation	
	Guidelines for SECNET 11 Local Area Networks in U.S. Army	
	Fixed Facilities and Systems (MMN 20073381)	.Att 1-1
Attachment 2.	E-Mail, 7 th Signal Command, BG Napper, Subject: Waiver for Use of Epoxy On PDS, 23 October 2009	. Att 2-1
Attachment 3.	Memorandum, USAF Judge Advocate, Subject: Medical Use of Encrypted Phone Systems and SIPRNET, 14 April 2004	.Att 3-1
Attachment 4.	E-Mail, GSA, Mr. Pollock, Subject: QPL for Combination Padlocks and E3 Class, 4 May 2010	. Att 4-1
Attachment 5.	E-Mail, NSA CISSP, Mr. Zundel, Subject: CNSSP 10 and CNSSI 4005, 27 May 2010	. Att 5-1
Attachment 6.	Figure 2, DOD Customer Connection Process, From the DISA Connection Process Guide, May 2010	.Att 6-1
Attachment 7.	Appendix F, DVS, From the DISA Connection Process Guide, May 2010	.Att 7-1
Attachment 8.	Appendix J, SIPRNET, From DISN Connection Process Guide, 22 June 2009	.Att 8-1
Attachment 9.	White Paper, Nova Datacom, Department of Defense Certification and Accreditation Process (DIACAP), 2009	.Att 9-1

Trade Name Disclaimer

The use of trade names and references to specific equipment in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report, in presenting the success or failure of one (or several) part number(s), model(s), under specific environment and output requirements, does not imply that other products not herein reported on are either inferior or superior.

This document may not be cited for advertising purposes.

SUMMARY OF CHANGES

Changes for Version 6

Updated all sections to current regulations and policies, reorganized all sections.

Updated, replaced, or added appendices and attachments.

vii

This page intentionally left blank.

SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) TECHNICAL IMPLEMENTATION CRITERIA

1.0 INTRODUCTION

1.1 Purpose

1.1.1 This document replaces the previous edition, titled *Technical Guide for the Integration of the Secret Internet Protocol Router Network (SIPRNET), Version 5.0*, August 2008.

1.1.2 The purpose of this document is to provide a set of criteria, culled from numerous Government regulations, policies, and standards, into one document with the intent of assisting a communications service provider, such as the Network Enterprise Center (NEC) on an Army installation, in planning, designing, and installing or expanding a SIPRNET capability for its users/tenants.

1.2 Scope

1.2.1 This document is not intended to replace any guidance given in any Government regulation, policy, standard, or other official documentation, nor relieve users of the responsibility to ensure their design and installation meets those regulatory requirements. This document incorporates information from the referenced regulations, policies, and standards (see Section 2) current as of the time of publication of this document. It is incumbent upon the user of this document to ensure they are familiar with any changes to the regulations, policies, and standards referenced that may have been made after the publication of this document. At the same time, the installation of a SIPRNET project that follows the criteria described herein will also meet the criteria published in the references, which is required for accreditation prior to operational use of the system.

1.2.2 Although this document may contain some information that may be useful in the Outside Continental United States (OCONUS) environment, the exact specifications and requirements in that theater may differ from the Continental United States (CONUS) theater. This document is not intended for use as technical criteria for OCONUS implementation. Likewise, this document is not intended for use as technical criteria for classified network implementation in a tactical environment.

1.3 SIPRNET Project Goal

1.3.1 The primary goal of a typical SIPRNET project is the expansion of the classified network RED-side infrastructure, extending connectivity to users not collocated with the SIPRNET distribution node or point of presence (PoP). The methodology used to provide the SIPRNET service will vary based upon such factors as the number of users, their relative locations and concentrations, building layout and construction, operational requirements, and design requirements/limitations imposed by higher headquarters or funding limitations.

1.3.2 Several standard designs have been developed and are discussed in more detail in <u>Section 4</u>. These designs are intended for use as a guideline and must be tailored to meet unique requirements at each location.

1.4 Disclaimer

1.4.1 The use of trade names and references to specific makes or models of equipment in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. This document, in presenting the success or failure of any model or part number, under specific environment and input/output requirements, does not imply that other products not herein mentioned are either inferior or superior.

1.4.2 This document may not be cited for advertising purposes.

1.5 Mandatory and Advisory Terminology

1.5.1 Two categories of criteria, mandatory and advisory, are used throughout this document, and are defined in the following paragraphs.

1.5.2 The use of the term "shall" indicates an imperative. It means that the criteria or action described is mandatory. In the context of this document, failure to meet the criteria or perform the action will result in the SIPRNET project being unsatisfactory, not meeting the minimum standards, and being unable to be accredited for use.

1.5.3 The use of the term "must" indicates that the criteria or action described, while advisory in nature, is highly recommended. It is a criteria or action that is expected to be met or followed. Failure to meet the criteria or perform the action will not result in the failure of the SIPRNET project, but it will degrade it and may result in the project not being able to be accredited.

1.5.4 The use of the term "should" indicates that the criteria or action described, while advisory in nature, is recommended. It is a criteria or action that is expected to be met or followed unless inappropriate for the particular circumstances at a specific site for a specific project. Failure to meet the criteria or perform the action will not result in the failure of the SIPRNET project, but it may degrade it and make it more difficult to achieve accreditation for use.

1.5.5 The use of the term "will" indicates that the action described applies to a Government agency and that this action will be accomplished if the circumstances warrant or allow.

2.0 REFERENCES

Note: The version in effect at the time of publication of this document shall apply.

2.1 National Security Agency (NSA) Publications

a. Committee on National Security Systems [CNSS] Instruction (CNSSI) 4009, *National Information Assurance (IA) Glossary*, 26 April 2010.

http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

b. CNSS Policy (CNSSP) 10, *National Policy Governing Use of Approved Security Containers in Information Systems Security Applications*, 16 December 2004 (U). (Note that this reference will be shortly superseded by CNSSI 4005.)

c. E-mail, NSA, CISSP, Mr. Zundel, 27 May 2010, Subject: CNSSP 10 and CNSSI 4005.

d. CNSS Policy 19, National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products, February 2007.

http://www.cnss.gov/Assets/pdf/CNSSP-19.pdf

e. CNSS, Index of National Security Systems Issuances, May 2010. http://www.cnss.gov/Assets/pdf/CNSS-INDEX.pdf

f. CNSSI 3021, Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD), September 2002 (U/FOUO).

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

g. Memorandum, SELCL-ID-P3, Subject: U.S. Army Implementation of CNSS Instruction No. 3021, Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD), 18 February 2003.

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

h. CNSSI 3029, Operational Systems Security Doctrine for TACLANE (KG-175), May 2004 (U/FOUO).

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

i. CNSS 057-06, Changes for CNSS Instruction No. 3029, 2006 Apr 19, (U/FOUO).

j. Memorandum, SELCL-ID-P3, Subject: U.S. Army Implementation of CNSS Instruction No. 3029, Operational Security Doctrine for the TACLANE (KG-175), 22 June 2004.

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

k. Memorandum, NSA, Subject: Notification of MANDATORY Field Software Upgrade (FSU) to all TACLANE-Micro KG-175D In-Line Network Encryptors (INEs), July 2008.

1. IDOC-007-04, Operational Security Doctrine for the KIK-20 Secure Data Transfer Device 2000 System (SDS) and the AN/PYQ-10 (C) Simple Key Loader (SKL) with the Embedded KOV-21 Cryptographic Card, July 2005.

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

m. Memorandum, SELCL-ID-P3, Subject: U.S. Army Implementation of Interim Operational Security Doctrine (IOSD) for the KIK-20 Secure Data Transfer Device 2000 System (SDS) and the AN/PYQ-10 (C) Simple Key Loader (SKL) with the Embedded KOV-21 Cryptographic Card, IDOC-007-04.

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

n. IDOC-009-06; Interim Operational System Security Doctrine for the TACLANE-GigE KG-175A, September 2006 (U/FOUO).

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

o. Memorandum, SELCL-ID-P3, Subject: U.S. Army Implementation of IDOC-009-06, Interim Operational Security Doctrine for the TACLANE-GigE KG-175A, 6 February 2008 (U/FOUO).

https://csla.army.mil/Sections/COMSEC/DocNSA.aspx

p. DOC-016-07, *Operational Security Doctrine for the Talon Cryptographic Token* (*TCT*) KOV-26, 11 January 2008 (U/FOUO).

q. IDOC-017-06, Interim Operational Security Doctrine for the SecNet-54 Secure Wireless 802.11 a/b/g Local Area Network (SWLAN) Encryptor, September 2006 (U/FOUO).

r. Memorandum, SELCL-ID-P3, Subject: Interim Operational Security Doctrine for the SecNet-54 Wireless Local Area Network, IDOC-017-06, 14 August 2007 (FOUO).

s. CNSSI 3032, Operational Security Doctrine for the VIASAT Internet Protocol (VIP) Crypto Version 1 (KIV-21), August 2003 (U/FOUO).

t. CNSSI 3035, Operational Security Doctrine for the RedEagle KG-245 In-Line Network Encryptor (INE), March 2007 (U/FOUO).

u. National Security Telecommunications and Information Systems Security Committee (NSTISSC) Advisory Memorandum (NSTISSAM), TEMPEST/2-95, *RED/BLACK Installation Guidelines*, 12 December 1995.

http://cryptome.org/tempest-2-95.htm

- v. NSTISSAM TEMPEST/2-95A, Amendment to TEMPEST 2-95, 03 February 2000.
- w. NSTISSI 7003, *Protective Distribution Systems (PDS)*, 13 December 1996 (U). http://www.cnss.gov/Assets/pdf/nstissi_7003.pdf

2.2 Department of Defense (DOD) Publications

a. DOD Regulation 5200.08-R, *Physical Security Program*, 9 April 2007, with Change 1, 27 May 2009.

http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf

b. DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), 23 April 2007.

http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

c. DOD Instruction 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies,* 3 November 2009.

http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf

d. DOD Instruction 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007.

e. Military Handbook (MIL-HDBK)-1013/1A, Design Guidelines for Physical Security of Facilities, 15 December 1993.

http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf

f. Military Standard (MIL-STD) 188-114, Revision A, *Electrical Characteristics of Digital Interface Circuits*, September 1985 (with Notice 1, December 1991).

 $http://www.everyspec.com/MIL-STD/MIL-STD+\%\,280100+-+0299\%\,29/MIL-STD-188-114A_21120/$

g. Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities, 9 July 2008.

http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf

h. *DOD Unified Capabilities Requirements 2010*, Section 5.3, Figure 5.3.1-14, ASLA UPS Power Requirements, 2010.

2.3 Defense Information Systems Agency (DISA) Publications

a. *Connection Process Guide, Ver. 3*, May 2010. http://www.disa.mil/connect

b. Circular 300-115-3, *Defense Information System Network (DISN) Secret Internet Protocol Routing Network (SIPRNet) Security Classification Guide*, 29 October 2009 (U/FOUO).

https://powhatan.iiie.disa.mil/disadocs/dc3001153.pdf

c. Access Control Security Technical Implementation Guide (STIG), Access Control in Support of Information Systems, Version 2, Release 2, 26 December 2008.

http://iase.disa.mil/stigs/stig/access_control_stig_v2r2_final_26_dec_2008.pdf

d. Defense Switched Network (DSN) STIG, DOD Telecommunications and Defense Switched Network Security Technical Implementation Guide, Version 2, Release 3, 30 April 2006.

http://iase.disa.mil/stigs/stig/dsn-stig-v2r3.pdf

e. Enclave STIG, Enclave Security Technical Implementation Guide, Version 4, Release 2, 10 March 2008.

http://iase.disa.mil/stigs/stig/enclave_stigv4r2.pdf

f. Network Infrastructure STIG, Network Infrastructure Security Technical Implementation Guide, Version 8 Release 2, 25 June 2010.

http://iase.disa.mil/stigs/content_pages/network_infrastructure.html

g. VVoIP STIG, Voice and Video over Internet Protocol (VVoIP), Version 3, Release 1, 23 December 2009.

http://iase.disa.mil/stigs/stig/index.html

h. VTC STIG, Video TeleConference Security Technical Implementation Guide, Version 1, Release 1, 8 January 2008.

http://iase.disa.mil/stigs/stig/vtc_stig_v1r1_010807_final.pdf

i. Wireless STIG, Wireless Security Technical Implementation Guide, Version 6, Release 2, 23 April 2010.

http://iase.disa.mil/stigs/stig/index.html

j. Defense Red Switch Network (DRSN) VoSIP Connection Guide, 4 May 2009

k. Memorandum, DISA Network Services, Subject: *Process for Use of Site Support Task*, 5 October 2008.

2.4 Department of the Army (DA) Publications

a. Army Regulation (AR) 25-1, Army Knowledge Management and Information Technology, 4 December 2008.

http://www.army.mil/usapa/epubs/pdf/r25_1.pdf

b. AR 25-2, *Information Assurance*, 24 October 2007, Rapid Action Review, 23 March 2009.

http://www.apd.army.mil/pdffiles/r25_2.pdf

- c. AR 190-13, *The Army Physical Security Program*, 30 September 1993. http://www.army.mil/usapa/epubs/pdf/r190_13.pdf
- d. AR 190-16, *Military Police Physical Security*, 31 May 1991. http://www.army.mil/usapa/epubs/pdf/r190_16.pdf

e. AR 380-5, *Department of the Army Information Security Program*, 29 September 2000.

http://www.army.mil/usapa/epubs/pdf/r380_5.pdf

f. AR 380-27, Control of Compromising Emanations, 19 May 2010.

http://www.army.mil/usapa/epubs/380_Series_Collection_1.html

g. AR 420-1, Army Facilities Management, Chapter 4, Army Military Construction and Non-Appropriated-Funded Construction Program Development and Execution, 12 February 2008.

http://www.apd.army.mil/pdffiles/r420_1.pdf

h. DA Pam 415-28, *Guide to Army Real Property Category Codes*, 11 April 2006. http://www.army.mil/usapa/epubs/pdf/p415_28.pdf

i. Defense Finance and Accounting Service (DFAS) Manual 37-100-10, *The Army Management Structure Fiscal Year 2010*, August 2009

http://asafm.army.mil/offices/BU/Dfas37100.aspx?OfficeCode=1200

j. Technical Bulletin (TB) 380-41, *Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material*, 9 March 2006.

https://csla.army.mil/Sections/COMSEC/DocArmy.aspx?fileID=69

(Requires Army Knowledge Online (AKO) login to CSLA website.)

k. Memorandum, DAMI-CD, Subject: Army Responsibilities for Protected Distribution Systems, 16 August 2007.

1. Memorandum (Draft), SAIS-AOI, Subject: Army Thin Client Computing Guidance, May 2010.

2.5 Miscellaneous Publications

a. U.S. Army Information Systems Engineering Command (USAISEC), Fort Detrick Engineering Directorate (FDED), *Technical Criteria for the Installation Information Infrastructure Architecture*, February 2010.

b. USAISEC, Technology Integration Center (TIC), TR No. AMSEL-IE-TI 07-063, *Design Guide for the Implementation of Wireless Technologies*, May 2007.

c. U.S. Army Network Enterprise Technology Command (NETCOM), NETC-ES-I, *The Army's FY09 Cryptographic Modernization Execution Plan v1.0*, 15 December 2008.

d. NETCOM 09-EC-M-0010, Best Business Practices (BBP), Wireless Security Standards, Version 3.0, 2 January 2009.

e. American National Standards Institute/Telecommunications Industry Association/ (ANSI/TIA) 607-A-2002, *Standard Commercial Building Grounding (Earthing) and Bonding Requirements For Telecommunications*, 22 October 2002.

f. Electronic Industries Alliance (EIA)-530, *High Speed 25 Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector*, May 26, 1992.

g. EIA-644, *Electrical Characteristics of Low Voltage Differential Signaling (LVDS) Interface Circuits*, 1 February 2001.

h. National Fire Protection Association (NFPA) 70, National Electrical Code, 2008.

i. Memorandum, Headquarters (HQ), U.S. Air Force/Judge Advocate, Subject: *Medical Use of Encrypted Phone Systems and SIPRNET*, 14 April 2004.

j. General Services Administration (GSA) Federal Specification FF-P-110J, *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack),* 11 February 1997.

k. GSA Federal Specification FF-P-110J Amendment 1, *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)*, 20 January 2004

l. E-mail, GSA, Mr. Pollock, Subject: *QPL for Combination Padlocks and e3 class*, 4 May 2010.

m. GSA Federal Specification FF-L-2740A, *Locks, Combination*, 12 January 1997. http://www.gsa.gov/graphics/fas/Ff12740a_R2FIBX_0Z5RDZ-i34K-pR.pdf

n. GSA Federal Specification FF-L-2740A, *Locks, Combination, 12 January 1997*; Amendment 1, 25 May 2001.

http://www.gsa.gov/graphics/fas/ff-1-2740amendment1_R2FIBX_0Z5RDZ-i34KpR.pdf

o. GSA Federal Qualified Products List, *Products Qualified Under Federal Specification FF-L-2740A*, *Locks, Combination*, 10 July 2002.

http://www.gsa.gov/graphics/fas/QPL-FF-L-2740-8_R2FIBX_0Z5RDZ-i34K-pR.pdf

p. Communications Security Logistics Agency (CSLA) paper, COMSEC 101, A Survival Guide for Communications Security, September 2009.

https://csla.army.mil/doc/COMSEC%20101.docx

(Requires AKO login to CSLA website.)

q. E-mail, 7th Signal Command, BG Napper, 23 October 2009, Subject: *Waiver for the use of Epoxy on PDS*.

r. Draft Memorandum, Army Certified TEMPEST Technical Authority (CTTA), Subject: Updated Installation Guidelines for SECNET 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20073381).

s. DFAS Manual 37-100-09, Subject: *The Army Management Structure, Appendix A, Expense/Investment Criteria*, August 2008.

3.0 MAJOR PARTICIPANTS AND RESPONSIBILITIES

3.1 U.S. Army Information Systems Engineering Command (USAISEC)

3.1.1 USAISEC serves as one of the Army's major communications engineering and implementation organizations and offers its services to DOD agencies on a reimbursable basis. Services range from performance of site surveys, development of the Technical Analysis and Cost Estimate (TA/CE) with List of Materials (LOM), procurement of materials, implementation and configuration of systems, and testing of completed installations.

3.1.2 In order to ensure that all information is gathered in an organized and complete manner, USAISEC has adopted the use of a Site Survey Checklist to help ensure all required information is obtained during the site survey for a SIPRNET expansion project. A sample checklist, attached in <u>Appendix D</u>, is provided as an example of the type of information that should be gathered to design a SIPRNET implementation. It is not an all inclusive list, as each design at each individual site has unique requirements. Additional information that affects the design will have to be gathered by the surveyor to ensure the design is implemented per all applicable criteria.

3.2 Designated Approving Authority (DAA)

3.2.1 The DAA at an Army post may be the Signal Brigade Commander (normally an O-6/Colonel position), with the establishment of the 7th Signal Command. In other cases the DAA is at the General Officer/Senior Executive Service level. Regardless, the DAA must be a United States citizen and an O-6/civilian equivalent or higher.¹

3.2.2 The DAA is responsible for ensuring all information systems (ISs) are properly certified and accredited.² They are also responsible for approving all local connections to the campus area network (CAN) at the site.

3.2.3 In association with approval, the DAA legally accepts any unmitigated risk associated with the system.

3.2 NEC / Communications Provider

3.3.1 The NEC is responsible for obtaining all systems accreditation.

¹ CJCSI 6211.02C, Enclosure B, Para 9.c(1), page B-11.

² CJCSI 6211.02C, Enclosure B, Para 14, page B-18.

3.3.2 The NEC is responsible for obtaining the technical review of all PDSs from the Army CTTA, as applicable. USAISEC will assist the NEC through the provision of any engineering documents developed by USAISEC.

3.3.3 The NEC will provide the required RED-side Internet Protocol (IP) addresses. This includes the procurement of any new IP subnets, as required.

3.3.4 The NEC is responsible for configuration of the existing CAN to pass encrypted classified network service to remote buildings, as required, if such service is tunneled through the CAN.

3.3.5 The NEC is responsible for ensuring that BLACK-side connectivity through the facility local area network (LAN) and the post CAN is available for all encryption devices, as required.

3.3.6 The NEC is responsible for the implementation of any new circuits required for the installation or expansion of a classified network service.

3.3.7 The NEC is responsible for the procurement of encryption devices through the CSLA and coordination with the local Communications Security (COMSEC) Custodian.

3.3.8 The NEC is responsible for coordinating with the COMSEC Custodian for the procurement and issue of encryption key material and key material loading devices.

3.3.9 The NEC Information Assurance Manager (IAM) is responsible for the overall security of the network. Items will include security oversight, vulnerability assessments, IA Vulnerability Alert (IAVA) compliance roll-ups, as well as other areas.

3.3.10 The NEC, in conjunction with the Information Management Officers (IMOs), is responsible for the procurement, installation, and configuration of application software to be installed on end-user computer resources.

3.3.11 The NEC is responsible for coordination with the Directorate of Public Works (DPW) in the completion of any agreements for site preparation issues (space, power, outlet locations, etc.).

3.3.12 If the classified network being installed is not on a military installation where common user services are provided by the NEC, then these responsibilities are those of the communications service provider for that facility.

3.4 Local Site / User / Tenant IMO

3.4.1 The IMO in each location is responsible for maintaining the physical and information security of the classified network access.

3.4.2 The IMO is responsible for providing all requested information to the NEC to enable the accreditation of the system.

3.4.3 The IMO is responsible for ensuring only the proper equipment is used on the classified network connections. The IMO is also responsible for ensuring equipment is properly marked with the classification of the network and is properly stored in approved security containers during non-duty hours unless they are located in an approved open storage area.

3.4.4 The IMO, in conjunction with the NEC/Service Provider, is responsible for the procurement, installation, and configuration of application software to be installed on end-user computer resources.

3.4.5 The IMO, in coordination with the NEC/Service Provider, is responsible for updating the applications and the installation of all software patches.

3.5 Army CTTA

3.5.1 The Army CTTA is responsible for ensuring all PDSs are installed, operated, and maintained, and all pertinent TEMPEST countermeasures are incorporated, in accordance with (IAW) all applicable regulations. This is accomplished by its technical review of all PDSs through the PDS approval process (see <u>Paragraph 5.2.2</u>).

3.5.2 The Army CTTA is also responsible for determining whether any TEMPEST countermeasures apply.

3.5.3 The Army CTTA is responsible for advising the DAA on all technical matters pertaining to TEMPEST issues and to a PDS.

3.6 Joint

3.6.1 The NEC, IMO, and tenant must coordinate the extension of the SIPRNET drops, ordering of equipment, and overall accountability for the system. To assist with responsibilities, requirements, and documentation, <u>Appendix G</u> includes an example of a Standing Operating Procedure (SOP) for SIPRNET at a given location.

3.6.2 The NEC, IMO, and tenant must coordinate closely with each other to ensure all of the appropriate physical security and operating procedures are implemented in order for the system to be accredited.

4.0 TECHNICAL SOLUTIONS DESCRIPTION AND CRITERIA

4.1 SIPRNET Programs

4.1.1 General

a. There are several standard programs under which many SIPRNET expansions are being accomplished. These programs are discussed in subsequent paragraphs. The technical methodology used to provide SIPRNET service under each program varies with the requirements at each site.

b. Although the standard programs provide SIPRNET access services in many cases, they are not all inclusive. There are other, smaller programs, as well as individual site specific projects, that can provide SIPRNET access services to an installation, tenant, or remote unit.

4.1.2 Brigade Combat Teams (BCTs) Implementation

a. The initial BCT effort expanded the SIPRNET access capability on a post for the BCTs. It installed service from an existing SIPRNET distribution PoP operated by the NEC on the installation to the BCT tenant buildings. The standard principle for the BCT SIPRNET expansion was:

- Light BCT: 7 buildings with connections for 48 users total.
- Heavy BCT: 8 buildings, with connections for 56 users total.

• Stryker BCT: 10 buildings with connections for 72 users total.

b. The BCT program typically installs SIPRNET in a distributed user fashion, with individual user drop boxes (UDBs), each containing one or more user connections (i.e., network jacks), providing SIPRNET access to the users.

4.1.3 Base Realignment and Closure (BRAC)

a. As a general rule, new construction under BRAC installs the same level of SIPRNET access in the new building as exists in the facility that a unit will be leaving. BRAC does not provide communications capabilities in the new facility/location that do not exist in the old facility/location.

b. In some cases, to allow for modernization and locally planned expansions that are cancelled due to a pending BRAC relocation, up to a 20 percent increase in capability may be authorized in the new facility/location. The defining guidelines for the new capability will be determined during the site survey and the development of the communications design.

4.1.4 Installation Information Infrastructure Modernization Program (I3MP)

a. In Fiscal Year (FY)07-FY09, I3MP included some limited SIPRNET design in its projects. These efforts typically installed SIPRNET access using the guidelines shown in Appendix E and Appendix F.

b. The I3MP SIPRNET projects included engineering and installation to the Brigadeand Battalion-level, focusing mainly on the BCTs, supporting brigades, and associated HQ. For installation of SIPRNET in existing facilities, the quantities of user drops provided is not as robust as for new construction.

4.1.5 Military Construction – Army (MCA)

a. Beginning with FY08-funded projects, MCA has included more extensive design and installation of SIPRNET drops. SIPRNET will be installed in most, but not all, buildings (see <u>Appendix F</u>).

b. As a general rule, all private offices will receive one SIPRNET drop. Design and use of "SIPRNET Cafés" (see <u>Paragraph 4.5.4</u>) is highly encouraged to accommodate the "occasional" SIPRNET user group. SIPRNET user drops will be designed for approximately 25 percent of the general population.

4.1.6 U.S. Army Reserve (USAR) SIPRNET to Battalion Program

a. Under this program, the USAR is providing SIPRNET service to its facilities with Battalion or above sized units. All of the USAR units in the facility, regardless of its command level, are allowed the use of the SIPRNET service, with proper security clearances.

b. The USAR is a common services provider with its "tenants" being distributed over a large geographical area. The majority of the USAR Centers are located not on military installations, but in commercial and residential areas of a city or county. Thus, the limited control area (LCA) around the building for the off-post USAR Centers is much smaller than for locations on-post.

SIPRNET Technical Implementation Criteria October 2010

c. To make up for the smaller LCA, the USAR Command is installing the SIPRNET service using the café concept, with stricter physical security requirements than would be required in an on-post environment. Each café is provided with either 6 or 10 user drops with 2 connections in each of 3 or 5 outlet locations. The use of the café concept in a common user area vice a particular unit's operational area (such as the S2 or S3) allows SIPRNET access by any unit in the facility at any time without impacting the operations of any other unit. The SIPRNET Café solution is described in more detail in Paragraph 4.5.4.

4.1.7 General Guidance for Building Rehabilitation and Retrofit

a. Numerous profiles for installation of SIPRNET in existing facilities are included in the tables provided in <u>Appendix E</u> for use as general guidance in design and estimation. The quantities in the tables reflect the guidelines from the Command, Control, Communications, Computers, and Information Management (C4IM) Service List.

b. For buildings that do not fit into the profiles in <u>Appendix E</u>, up to five SIPRNET drops will be engineered and installed for those buildings accommodating personnel in the grade/rank of O-5/Lieutenant Colonel and above, or the civilian equivalent, with command responsibilities.

4.1.8 Medical Facilities

a. Hospitals and medical facilities will be provided only one SIPRNET drop per building due to Geneva Convention and Law of Armed Conflict (LOAC) issues. This same restriction applies to new medical facility construction as well (see category 510 in Appendix F).

b. The SIPRNET access in medical facilities may only be used for the exclusive purpose of medical operations³.

4.2 Connectivity Areas of Responsibility

4.2.1 General

a. The implementation of SIPRNET access spans from the individual user up to the global SIPRNET wide area network (WAN). The responsibilities for operating, maintaining, and implementing such access can be divided into three main areas of responsibility, each by a different organization: DISA, NEC, and tenant/user.

³ Memorandum, U.S. Air Force Judge Advocate, 14 April 2004.

b. The areas of responsibility between the three agencies correspond roughly to the size of the network: WAN, metropolitan area network (MAN)/CAN, LAN. See Figure A-1 for a depiction of the various sized networks and how they interrelate.

c. Each of the three main areas of responsibility must be addressed for a successful implementation of SIPRNET access. <u>Figure A-2</u> depicts a high level view of the overall user to WAN reach of the SIPRNET with the three areas of responsibility delineated.

4.2.2 DISA-Managed

a. <u>Figure A-3</u> shows an expanded view of the DISA-managed portion of the SIPRNET. This drawing represents a composite of multiple design options and will not apply to every situation. It is intended to give the reader a conceptual view of various configurations, architectures, and security designs as described in the ARs, STIGs, and other policy documents.

b. As the circuit bringing SIPRNET access into the post is managed and controlled by DISA, all of the equipment associated with it is also managed by DISA. Although controlled by DISA, the near-end equipment used to terminate the circuit at the post is located in one of the NEC facilities on post. Figure A-3 does not show an all inclusive list of equipment, but only a representation of the type equipment.

c. As indicated in Figure A-3, SIPRNET traffic is delivered from the DISA cloud, through the local DISA PoP and COMSEC, to the NEC SIPRNET PoP using a variety of transmission methodologies ranging from point-to-point serial circuits to fiber optic Synchronous Optical Networking (SONET) channels. When providing SIPRNET connectivity to a post, DISA will provide the proper circuit for the bandwidth requested. The requesting agency, in this case the NEC, must fund all costs associated with the provisioning of the circuit, including equipment and labor costs for equipment installed at both ends of the circuit. In lieu of providing the funding, the circuit requesting agency may elect to provide the equipment directly to DISA.⁴ Funding will still have to be provided to DISA for the related installation costs, and the equipment must be that specified by DISA during its circuit engineering process.

d. The circuit conditioning equipment and encryption device are typically located on the post in an NEC-controlled facility, even though they are DISA assets. The demarcation line between DISA and NEC responsibilities is typically the RED-side connection on the encryption device used between the SIPRNET WAN and the NEC-controlled equipment.

⁴ DISA Memorandum, Process for Use of Site Support Task, Enclosure 1, Para 4.

4.2.3 NEC-Managed

a. <u>Figure A-4</u> shows an expanded view of the NEC-managed portion of its SIPRNET connectivity. This drawing represents a composite of multiple design options and will not apply to every situation. It is intended to give the reader a conceptual view of various configurations, architectures, and security designs as described in the ARs, STIGs, and other policy documents.

b. As indicated in Figure A-4, between the RED-side of the DISA-controlled encryption device and the SIPRNET PoP distribution router, there is a suite of network security equipment. The actual type, quantity, and configuration of the equipment will be determined by the local NEC (per DISA policy⁵) as it is responsible for the network security of everything behind the RED-side of the encryption device (termed an "enclave" from the WAN perspective of DISA). Collectively, the routers, firewalls, and other equipment are referred to as the NEC SIPRNET PoP. The extension of SIPRNET service to tenants/users from the SIPRNET PoP is the main concern of the majority of SIPRNET expansion projects and this document. Following are four basic scenarios for these SIPRNET expansion projects:

(1) Scenario 1. The first and most common scenario is the military installation where an NEC (or other service provider) has a SIPRNET PoP and uses the existing CAN for extending the service to the tenant/user that is also located on the military installation. Although this scenario will cover the majority of implementations, other solutions may be required to meet the tenants' exact mission needs.

(2) Scenario 2. In the second scenario, a remote user that is not on the military installation needs SIPRNET service from an existing SIPRNET PoP on the military installation (i.e., an off-post extension). Typically, this scenario involves a small user group (1-20 users), but may be employed for larger groups.

(a) In this scenario, the physical security requirements for the SIPRNET network equipment located at the remote user location must be considered. The type of network security equipment required must be coordinated with the SIPRNET service provider (such as the NEC on the military installation where the circuit will originate).

(b) Although this scenario involves a local off-post circuit extension under the control of the NEC, it must be coordinated with the DISA Connection Approval Office

⁵ DISA Network Infrastructure STIG, Section 2.1.

 $(CAO)^6$ prior to implementation to help ensure the accreditation of the entire NEC enclave will not be negatively impacted. As the local commercial WAN the off-post circuit traverses is not already encrypted, encryption devices must be used at each end of the circuit before it is handed off to the local commercial circuit provider.

(c) If or when DISA approves the extension of these services, the originating PoP (the NEC) provides and controls the address space used at the remote user location and is responsible for accounting (documenting the network configuration) for the certification of this new location. Note that the use of public IP address space (10.0.0.0, 172.16.0.0, 192.168.0.0) is not allowed on SIPRNETs.⁷

(3) Scenario 3. In the third scenario, the user requires SIPRNET access in a nonmilitary environment, such as in an off-post contractors facility. This scenario is similar to the previous scenario except for the affiliation of the remote user.

(a) Again, the user must address the physical security requirements for the SIPRNET network equipment that will be required at the user's location. The type of network security equipment required must be coordinated with the SIPRNET service provider (such as the NEC on the military installation where the circuit will originate).

(b) As the remote user is not a military or Government unit, the SIPRNET connection must be sponsored by a Government agency.⁸

(4) Scenario 4. In the fourth scenario, the user needs a SIPRNET dial-up capability for limited use by a very small group of users.

(a) Dial-up SIPRNET is an inexpensive means to provide SIPRNET access to those who require service using commercial telephone lines. Access is provided by dialing into the DISA communications server using a Secure Data Device (SDD)-1910, Secure Telephone Unit (STU), or Secure Terminal Equipment (STE).

(b) If dial-up service is required, the user should coordinate directly with DISA. Dial-up access is restricted to Government or military personnel only. It is not available for contractor personnel.

(c) <u>Figure A-6</u> depicts a simplified account of a dial-up connection from the tenant to the DISA server.

⁶ DISA Network Infrastructure STIG, Section 2.3.

⁷ DISA Network Infrastructure STIG, Section 2.8.

⁸ DISN Connection Process Guide, Paragraph 2.1 and Enclosure C.

c. Post Transport.

(1) Although encryption devices will be required in most situations, connectivity between the NEC SIPRNET PoP and the remote user location may be provided in various ways. Three of the more prevalent methods of connectivity are noted in the following subparagraphs:

(a) Alternative 1 – Traversing over the existing CAN. The SIPRNET circuit may traverse from the NEC PoP to each end user building (EUB) over the existing CAN infrastructure in encrypted (BLACK) form. This is referred to as tunneling, and is discussed in more detail in <u>Paragraph 4.6</u>. This is the preferred method of inter-building transport.

(b) Alternative 2 – Dedicated Cable Path. Dedicated cable pairs, either copper or fiber, may be used to extend SIPRNET service in the encrypted (BLACK) form. This method does not utilize the post cable infrastructure in an efficient manner, so it is not the preferred method. As the information is encrypted, the use of a PDS is not required.

(c) Alternative 3 – Exterior PDS. As the information being transmitted is not encrypted (it is RED, or plain text), a PDS is required. An exterior PDS⁹ between buildings is an expensive method for inter-building transport, especially if there are multiple buildings or the buildings are not immediately adjacent to each other. The SIPRNET service is extended in unencrypted (RED) form, eliminating the cost of the COMSEC devices. However, the cost of the PDS will more than offset the COMSEC savings in most cases. At the same time, additional physical security checks and procedures are required to ensure the exterior PDS remains secure. For these reasons, exterior hardened PDS is not a preferred method of transport between buildings.

4.2.4 Tenant/Local/User-Managed

a. <u>Figure A-5</u> shows an expanded tenant/user-managed portion of the SIPRNET connection drawing. It represents a composite of multiple design options and will not apply to every situation. It is intended to give a conceptual view of various configurations, architectures, and security designs as described in the NSTISSIS, ARs, STIGs, and other policy documents

b. A port on each building's post unclassified network switch (the EUB switch) will be reserved for the encrypted (BLACK) side of the encryption device. Where the device is collocated in the telecommunication room with the switch, the encryptors interface cable will be plugged directly into the reserved switch port. If the device is located in a room

⁹ NSTISSI 7003, Annex B Paragraph 4a(1)(d) and (e).

other than the telecommunications room, such as an office, encryptor BLACK connection will use the building's cable infrastructure to the telecommunications room and then be connected to the reserved switch port.

c. The RED tenant router is an optional requirement and is only needed if a virtual private network (VPN) is required to pass traffic between two RED enclaves separated by a pair of INEs and the traffic is of a type that does not get passed by the INE.

d. Distribution of the SIPRNET service from the switch to the users is normally done via a PDS of some type, dependent upon the physical locations it must traverse. This subject is discussed in more detail in Paragraph 4.4.

4.3 Access Areas and Threat Levels

4.3.1 General

a. There are basically three levels of access areas: controlled access area (CAA), LCA, and uncontrolled access area (UAA). There is also a special type of CAA, the open storage area. The differences between them are in the arena of physical security and access into the areas. The type of access area and the local threat environment determine the type of PDS and other supplemental security measures required to protect the classified information transiting the area¹⁰.

b. Local threat levels are designated as low, medium, or high. The exact designation of threat levels for each specific geographical area is contained in a classified NSA document (*Information Assurance Standoff Capabilities Report*) and is thus beyond the scope of this unclassified document. For a listing of the higher threat locations within CONUS, refer to the classified report.

4.3.2 Uncontrolled Access Area (UAA)

a. A UAA is an area over which no personnel access controls are or can be exercised.¹¹ In short, it is an area that is open to the public. There are no personnel controls that ensure only authorized personnel are allowed into the area, nor that those personnel entering the area have a security clearance. This is the least secure of the types of access areas.

b. A hardened PDS is required for the transmission of any and all unencrypted classified information through a UAA at any threat level.

¹⁰ NSTISSI 7003, Annex B Table B-1.

¹¹ NSTISSI 7003, Annex A Paragraph g.

4.3.3 Limited Controlled Area (LCA)

a. An LCA is an area with a PDS going through it where exploitation of the PDS is not considered likely or where legal authority to identify and remove a potential exploitation exists.¹²

b. If the area has some personnel access controls (i.e., it's not a UAA), yet does not meet the definition of a CAA, then it is an LCA. A Government or military facility with a locked door where a visitor, once admitted to the facility, can roam unescorted is an example of an LCA.

c. A hardened PDS is required for the transmission of any and all unencrypted classified information through an LCA at any threat level.

4.3.4 Controlled Access Area (CAA)

a. A CAA is an area in a facility that is under direct physical control within which unauthorized persons are denied unrestricted access. If they are granted access, they are then escorted by authorized persons or are under some form of continuous physical or electronic surveillance.¹³

b. By definition, a CAA is not necessarily an area rated for the open storage of classified material.

c. The use of a simple PDS in lieu of a hardened PDS in a CAA depends upon several other physical security and procedural issues, and must be closely coordinated with the proper local security personnel. If the CAA is not approved for open storage, it is highly recommended that a hardened PDS be used.

4.3.5 Open Storage Area

a. An open storage area is a secure room or vault that has met certain construction standards. An open storage area is a special case CAA in which classified material may be stored unattended outside of a GSA safe as the room itself provides the requisite physical security.

b. A PDS is not required inside an open storage area for classified information at or below the security level of the open storage area.

c. The preferred method of safeguarding classified material is secured inside a GSAapproved safe. Designation of an open storage area will only be approved when storage in

¹² NSTISSI 7003, Annex A Paragraph d.

¹³ NSTISSI 7003, Annex A Paragraph b.

GSA-approved safes is not feasible due to size, shape, or volume of the material stored.¹⁴ In short, the use of open storage areas is not the preferred method of securing classified material.

d. The commander is responsible for designating an area as restricted or controlled to safeguard property or resources, such as the classified material or information, for which the commander is responsible.¹⁵ To be designated as an open storage area, the selected area must be designated as such by the commander and meet the appropriate physical security standards. Along the approval process, a physical security inspection and/or a security engineering survey will need to be completed¹⁶. Upon successful completion of the inspection, and recommendation from the physical security personnel, the commander may designate in writing that an area is approved for open storage at a given classification level.

e. The physical security construction standards for an open storage room at the Secret level are as follows.¹⁷ In addition, an intrusion detection system (IDS) (i.e., an alarm system) is required to be used.¹⁸

(1) The floor, walls, and ceiling shall be made of permanent construction materials that offer resistance to, and evidence of, unauthorized entry into the area. In addition, the walls shall extend from the true floor to the true ceiling. The wall extensions may also be made with 18-gauge wire mesh or expanded steel screen if the permanent walls do not extend from true floor to true ceiling.

(2) The doors to the area shall be substantially constructed of wood or metal. Wood doors shall be solid throughout. The hinge pins of doors that swing outward from the area (i.e., the hinges are accessible from outside the area) shall be pinned, brazed, or spot welded to prevent its removal.

(3) The access door into the area shall be equipped with a combination lock such as the X08 or X09.¹⁹ Doors other than the access door shall be secured from inside the area to prevent entry from outside. Key operated locks that can be accessed from outside the area are not authorized.

¹⁴ AR 380-5, Paragraph 7-12.

¹⁵ DOD Reg 5200.08-R, Paragraph C3.2.4 and AR 190-13, Paragraph 6-3.

¹⁶ FM 3-19.30, Chapter 11.

¹⁷ AR 380-5, Section 7-13 Paragraph b and Section 7-20.

¹⁸ AR 380-5, Section 7-20 Paragraph e and Section 7-14.

¹⁹ Fed Spec FF-L-2740A with Amendment 1 and Fed Qualified Products List QPL-FF-L-2740-8.

SIPRNET Technical Implementation Criteria October 2010

(4) If there are windows in the secure area where the bottom of the window is less than 18 feet from the ground, or are easily accessible by an object nearby (such as a tree or fence), they shall be covered with materials to help prevent forced entry to a level at least equivalent to the exterior walls. Typically, metal bars or wire mesh screening is used to accomplish this. The method of securing the covering over the windows is part of the security system, so it shall also provide protection at least equivalent to the walls. In short, the fasteners shall be inaccessible from outside or be non-removable.

(5) Windows which might reasonably afford a view of the classified information inside the area shall be made opaque or be equipped with blinds, drapes, or other coverings.²⁰

(6) Any openings into the room, such as for air conditioning ducts or vents, are required to be less than 96 square inches. If larger than 96 square inches, the opening shall be hardened to resist penetration²¹. The methods used to harden the opening are basically to break it up into a number of smaller openings rather than cover it over or just reduce the size.²²

4.4 Protected Distribution Systems (PDS)

4.4.1 General

a. A PDS is a cable or carrier distribution system used to transmit unencrypted classified information through an area of lesser classification.²³ The type of PDS required is determined by the type of access area the PDS transits, as well as the local threat level. The less secure the access area is, and the higher the local threat level, the more physical security must be provided by the PDS to the classified carrier inside the PDS.²⁴ A basic principle is that if the room or area that the PDS is going through is not an open storage area rated for classified storage at or above the level of the classification of the information being carried inside the PDS, then a PDS is required.

b. As a system, the PDS includes all components from end to end, for the purposes of this document. The PDS begins with the security container housing the network equipment (COMSEC, switch, etc.) and ends with the wall-mounted box that holds the user access connections. The portion of the PDS in between, the part that carries the classified cabling

²⁰ AR 380-5, Section 7-20 Paragraph d(1).

²¹ AR 380-5, Section 7-13 Paragragh b(5).

²² Mil Hdbk 1013/1A, Paragraph 5.6.7

²³ NSTISSI 7003, Annex A Paragraph e.

²⁴ NSTISSI 7003, Table B-1.

from one are to another, is the carrier. These three main components are referred to as the <u>Building PoP</u>, the <u>PDS carrier</u> (also called the conduit or duct), and the <u>UDB</u>, each of which are discussed in more detail in <u>Paragraph 4.7</u>.

4.4.2 PDS Purpose

a. The purpose of a PDS is not to prevent penetration to the classified cabling inside the PDS (i.e., prevention), but rather to deter unauthorized access and to provide evidence of penetration or attempted penetration (i.e., detection).²⁵

b. The two basic types of PDSs; simple and hardened, are discussed in more detail in the following paragraphs. All PDSs fall into one of these two categories. Although the discussion tends to center around the carrier, the same requirements and guidance pertain to the PoP security housing and the UDBs at each end of the carrier.

4.4.3 Simple PDS

a. A simple PDS may be used for SIPRNET cabling as long as the PDS is contained inside a Confidential rated CAA (an <u>open storage area</u> rated at the Confidential level). In a Secret or higher rated <u>open storage area</u>, a PDS is not required.²⁶ Although a PDS is not required, a simple PDS should be installed to provide an orderly scheme to route the cables and to prevent the RED SIPRNET cables from accidentally becoming intermixed with any BLACK cables.²⁷

b. In a simple PDS, the cables must be in a carrier (i.e., a duct or conduit), but the carrier may be constructed of any material. However, the joints and access points should be secured and under the control of personnel cleared to the Secret level. ²⁸ In a Secret rated <u>open storage area</u>, a carrier must still be used, but it does not need to be sealed or controlled. The most common carrier in these cases, based on cost of materials and installation, is wall-mounted plastic duct.

4.4.4 Hardened PDS

a. General.

(1) A hardened PDS is required for SIPRNET cabling where the PDS transits an <u>LCA</u> or a <u>UAA</u>. It is also highly recommended inside a Confidential <u>open storage area</u>.

²⁵ NSTISSI 7003, Annex A Paragraph 2.

²⁶ NSTISSI 7003, Annex B Table B-1.

²⁷ NSTISSAM 2-95, Para 4.5.

²⁸ NSTISSI 7003, Annex B Paragraph 4.b(2).

SIPRNET Technical Implementation Criteria October 2010

(2) Three types of hardened PDSs; hardened carrier, continuously viewed carrier, and alarmed carrier, are discussed in the following paragraphs.

b. Hardened Carrier.

(1) A hardened carrier is the most common type of hardened PDS. It is so common, the term "hardened PDS" or just "PDS" is often mistakenly used in lieu of the term "hardened carrier." The hardened carrier shall be a ferrous metallic conduit or duct. The fittings and connectors shall be made of the same ferrous metal material. All seams and joints shall be completely sealed through welding, the use of high compression fittings, or epoxy. The covers of all access points, such as pull boxes or UDBs, shall likewise be sealed unless they are secured with a GSA-approved changeable combination padlock. Boxes with prepunched knockouts (e.g., National Electrical Manufacturers Association (NEMA) 1 hardware) are not authorized to be used.²⁹ The only changeable combination padlock currently approved by the GSA is the Sargent & Greenleaf model 8077.³⁰

(2) The hardened carrier most personnel are familiar with is electrical metallic tubing (EMT) conduit. When using EMT conduit, the fittings and connectors shall be made of the same ferrous metal. The cheaper "pot metal" type fittings are not permitted. Non-metallic fittings shall not be used in any hardened carrier system.

(3) Conduit is defined as a tube, duct, or protected trough for carrying wires or cabling. It may be round, square, or rectangular in shape. It most commonly is a closed system with only the ends being open for feeding cables through. However, it may also be the type with a removable cover, enabling cabling to be laid into, rather than pulled through, the conduit. The use of a hardened carrier with a removable cover allows the future addition of extra cables and expansion of the PDS (referred to as "future adds, moves, and changes") with minimal effort. This benefit is offset by the requirement to remove the sealing material from the carrier, which may also damage the carrier, which requires its replacement at added expense. For the conduit with a removable cover, the requirement to seal all joints and edges applies to the entire length of the removable cover, as well as to the edges and joints of the fittings. The extra labor involved in sealing both sides of a removable cover for the length of the entire hardened carrier makes this a more expensive solution than standard conduit such as EMT.

²⁹ NSTISSI 7003, Annex B Paragraph 4.a(1).

³⁰ E-mail, GSA, Mr. Christopher Pollock, 4 May 2010.

(4) The requirement to seal the carrier may be waived if approved by the DAA on a site by site basis through a risk acceptance by the DAA. The 7th Signal Command DAA has approved a conditional waiver where the hardened carrier does not need to be sealed.³¹ The sites covered by this waiver are included in the reference, and are the military installations (the NECs) that fall under the authority of the 7th Signal Command. As part of the PDS approval process by the Army CTTA, the DAA must still sign/approve a risk acceptance for each specific site. **Note:** Local physical security personnel may, at their discretion, override this waiver and require the use of epoxy to seal the PDS duct. It is always an option to increase the security measures. The conditions for the waiver, also listed in the reference, are as follows:

(a) The hardened carrier used shall be the ferrous steel raceway manufactured by Holocom.

(b) The proper top cap locking kits for the Holocom raceway shall be used in the design and installation.

(c) The Holocom raceway shall be installed by Holocom certified technicians.

(5) Although hardened carrier is typically used inside a building or facility, it may also be used to carry classified cabling between buildings. This is usually a cost prohibitive solution, especially when the PDS must be run between multiple buildings in a point-tomultipoint configuration such as from an NEC facility to multiple tenant buildings on a military installation. Hardened carrier installed between buildings may be buried or suspended.

(a) If buried, the hardened carrier shall be at least 1 meter below the surface on property owned or leased by the Government. If manholes are used in the carrier distribution system, they shall be secured using a GSA-approved changeable combination padlock. These requirements are for the low threat environments inside the U.S. only. For higher threat environments, or OCONUS locations, the hardened carrier shall be encased in at least 8 inches of concrete.³²

(b) If the hardened carrier is to be suspended between buildings, it shall be a minimum of 5 meters above the surface grade level, and the area the PDS traverses over

³¹ E-mail, 7th Sig Cmd, BG Napper, 23 October 2009.

³² NSTISSI 7003, Annex B Paragraph 4.a(1)(d).

SIPRNET Technical Implementation Criteria October 2010

shall be owned or leased by the Government. In addition, the area containing the PDS shall be illuminated to help deter tampering.³³

c. Continuously Viewed Carrier.

(1) A continuously viewed carrier is just that. It is a PDS carrier that must be under direct continuous observation 24 hours a day. There must be operational procedures in place to ensure all attempts to disturb the PDS are investigated by security personnel within 15 minutes.³⁴

(2) There is no restriction on the type of carrier, so it may be made of any material and does not need to be sealed, as it is a guarded system. The security afforded the classified cabling stems from the quick response by security personnel to any attempt to compromise the carrier.

d. Alarmed Carrier.

(1) An alarmed carrier is a carrier that is protected by an alarm system that is approved by the cognizant COMSEC and/or physical security authorities.³⁵ The use of an alarmed carrier as a hardened PDS must therefore be closely coordinated with these authorities from the design phase through the installation and certification phases. There is no distinction made as to whether the alarm system is internal or external to the carrier, just that the carrier be protected by one.

(2) An example of an alarmed carrier being protected by an external alarm system would be where the entire length of the PDS was protected by an IDS alarm system, such as the type used in secure open storage areas. This tends to be an expensive solution based on the normal size and branching routes that a PDS normally takes. However, alarming the space around the PDS does provide the side benefit of increasing the overall security posture of the area the PDS is installed in.

(3) An example of an alarmed carrier being protected by an internal alarm system would be where an electronic system is used to monitor and report on the status of the cables inside the carrier. This type of system monitors the physical layer (Open Systems Interconnection [OSI] Model Layer 1) of the data transmissions through a fiber optic cable, looking for variations in the timing and shape of the light pulses that are caused by vibrations as a result of an attempted break-in. By operating at the physical layer, the alarm

³³ NSTISSI 7003, Annex B Paragraph 4.a(e).

³⁴ NSTISSI 7003, Annex B Paragraph 4.a(3).

³⁵ NSTISSI 7003, Annex B Paragraph 4.a(2).

system does not capture, process, or record any classified data in the cable. Two examples of this type of fiber optic alarmed carrier are the Interceptor, manufactured by ((additional details are available at <u>www.gocsc.com/secureIT</u> or <u>www.networkintegritysystems.com</u>) and the SecureLAN by Fiber SenSys (additional details are available at <u>www.fibersensys.com</u>).

4.4.5 PDS Periodic Inspections

a. During its operational lifetime, a PDS must be periodically visually inspected for signs of penetration, tampering, or degradation.³⁶

b. For a PDS transiting a UAA or an LCA under the low threat environment in the U.S., the visual inspection shall be done at least once per day on a random schedule. This is also true for a Secret level (i.e., SIPRNET) PDS that traverses a Confidential rated open storage area.³⁷

c. To aid in the conduct of the visual inspection, the PDS shall not be installed in a concealed location such as inside walls, above suspended ceilings, or below raised flooring.

d. Inspection of the PDS must include the entire PDS, not just the carrier portion. It must be inspected from end to end, from the SIPRNET PoP security housing to the UDBs containing the user network access ports.

4.5 SIPRNET Physical Architecture

4.5.1 General

a. There are three basic physical architectures for the distribution of SIPRNET inside a facility, or EUB: <u>Distributed PDS</u>, <u>SIPRNET Café</u>, and <u>Individual COMSEC</u>. Each alternative offers different advantages and disadvantages in physical security, ease of operation, and cost.

b. Regardless of the physical architecture chosen, all implementations of SIPRNET must take into consideration the requirement to control compromising electromagnetic emanations, commonly referred to as TEMPEST.³⁸ The best time to address TEMPEST issues is during the design phase of the SIPRNET system.

c. Of particular concern for TEMPEST issues is the size of the inspectable space around SIPRNET assets and the type and location of all fixed radio frequency (RF)

³⁸ AR 380-27, Control of Compromising Emanations, 19 May 2010.

³⁶ NSTISSI 7003, Annex B Paragraph 1.a(6).

³⁷ NSTISSI 7003, Annex B Table B-2.

transmitters and antennas within 10 meters of RED processors.³⁹ While additional information is presented in <u>Paragraph 4.9.2(c)</u> of this document, further technical details regarding TEMPEST issues must be received from the Army CTTA, as they are often classified.

4.5.2 Installation and Design Considerations

a. General.

(1) The SIPRNET is a command and control (C2) system. As such, the reliability and availability of the user access to it must always be considered when designing and installing a SIPRNET system. These are typically higher than that afforded a non-C2 system such as Unclassified but Sensitive Internet Protocol Router Network (NIPRNET).

(2) As the SIPRNET is a classified system at the Secret level, physical security must be addressed during the design and installation of all SIPRNET access projects to help ensure the system can successfully pass the security inspection required for accreditation.

b. Alternating Current (AC) Power.

(1) One of the key aspects of keeping the SIPRNET access available to the end users is the AC power to all of the components. Regardless of its location, all of the devices and equipment used to provide SIPRNET access must have a reliable AC power source.

(2) In all locations where the equipment used for SIPRNET access provides service to multiple users, such as the installation PoP or a building PoP, the equipment shall be provided AC power from a dedicated circuit breaker. If the equipment is contained in multiple equipment racks, cabinets, or other type of security housing, each shall be provided AC power from a dedicated circuit breaker.⁴⁰ For redundancy, it is recommended that AC power be available from dual dedicated circuit breakers.

(3) At individual end user locations, where a loss of service due to a circuit breaker would only affect one user, dedicated circuit breakers are recommended based on whether or not the users function is considered mission critical/essential. For example, the commander, operations officer, and intelligence officer of a unit with SIPRNET access may need dedicated AC power for their SIPRNET access while other SIPRNET users in the unit do not.

³⁹ AR 380-27, Chapter 4, Paragraph 4-1.

⁴⁰ Technical Criteria for the Installation Information Infrastructure Architecture, Paragraph 2.5.1.5.

(4) For locations that provide SIPRNET access service to multiple users, such as the installation PoP or a building PoP, the equipment used to provide SIPRNET access shall be provided backup power in the form of an uninterruptible power supply (UPS). The UPS shall be sized to provide backup power for all of the equipment for at least two hours.⁴¹ Additional backup power time is highly recommended for equipment serving multiple users or high priority users. For individual users whose function is considered mission critical/essential, the use of a small UPS for their terminal equipment is recommended.

c. Power over Ethernet (PoE).

(1) PoE is a useful tool for reducing the footprint of the equipment for end users. It is an equipment capability built into some network switches that allows the switch to provide the operating power to an end user device, such as a wireless access point (WAP), a Voice over Secure Internet Protocol (VoSIP) phone, or other small device. PoE is not useful for providing power to end user computers or laptops. PoE is provided by the switch over the same network cabling that is used to provide network access, so no additional cabling is required. However, the end user device and the network switch must both be purchased with the built-in capability for PoE.

(2) When designing a SIPRNET system, the requirement for VoSIP must be considered (see <u>Paragraph 4.10</u>). If VoSIP is currently in use on the installation, the use of PoE must be designed into each building PoP. If VoSIP is not currently used, its future implementation should be accounted for. The total power the projected number of end user devices will consume should be used when planning the size and capabilities of the network switch to ensure the switch will be able to support the total number of planned.

(3) The secondary impacts of planning for PoE capability in a switch are UPS sizing and cooling. As a PoE capable switch consumes more AC power than a regular network switch, the UPS may have to be sized upwards slightly to maintain the proper amount of run time during an AC power outage. The additional AC power consumed by the PoE switch also generates more waste heat. In a closed environment, such as inside a closed equipment cabinet or information processing system (IPS) container, additional cooling capability may be needed as well.

4.5.3 Distributed PDS

a. A Distributed PDS is one where the PDS carrier is routed from the source (the distribution switch) to the destination (UDB locations) in a branching fashion. The top

⁴¹ UCR 2010, Section 5.3.1, Figure 5.3.1-14

portion of <u>Figure A-7</u> depicts an example of the Distributed PDS architecture with 11 users that require access to SIPRNET. Therefore, there are 11 UDBs, each containing 1 network connection for SIPRNET access. In some cases several of the UDBs may contain 2 connections if there are multiple users in a room or a requirement for a networked printer or other device.

b. The vast majority of facilities are not secured to open storage standards, so a hardened carrier PDS is required for a SIPRNET implementation using the distributed architecture. Due to the large amount of PDS material required in the distributed architecture, and the labor required to install it, the overall cost of the installation is relatively high.

c. On the operational side, users may access SIPRNET from their desk when SIPRNET access is required. This does not address the issues of where the classified laptops or hard drives will be stored when not in use though. It is impractical for users to have their own storage safe for their computer hardware and any classified documents or material they may have. Typically, there will be one central location containing the storage safe(s) that users will have to visit before and after using SIPRNET. It is only the actual usage time that is done at their desk.

d. From the operational security aspect, in the distributed architecture the security zone for the building is all of the areas where SIPRNET is used or transits through via the PDS. In a widely distributed architecture, the security zone could encompass almost the entire building. There may be several different types of access areas the PDS transits through in the security zone. Within the overall security zone, the PDS must be monitored and inspected according to the type of access areas that it goes through. At each of the user drop locations, care must be taken to ensure computer screens are properly oriented and shielded to prevent the unintentional displaying of classified material. Personnel must be aware of, and follow, the security procedures developed within this large security zone. As the SIPRNET architecture distributes throughout the building and the security zone increases in size, the potential for an inadvertent security violation increases.

e. In a large distributed PDS using copper LAN cabling, the effective cabling distance for Ethernet (100 meters) may sometimes be exceeded. To ensure all user access connections are within the Ethernet specifications, there are two solutions.

(1) One solution is to change the cabling for the distant user drops from copper to multimode fiber optic cabling, which has a much longer Ethernet distance (2 kilometers [km]). This requires different port types (fiber) on the building PoP switch as well as in the user computers. The other solution is the use of intermediate, or workgroup, switches along the PDS route to extend the effective Ethernet distance. These switches act as repeaters and multiplexers in that they regenerate the Ethernet signal, giving another 100 meters of "reach," and they "fanout" one signal cable from the building PoP to multiple distant users.

(2) When using intermediate switches, the switches must be afforded the same level of physical protection as the SIPRNET cabling inside the PDS, or better. In some cases, the intermediate switches may be placed inside a large wall-mounted PDS box someplace along the PDS carrier route. In other cases, an IPS container will need to be installed and the PDS carrier routed to/from it. The use of the IPS container is more expensive than the large PDS box. However, it does require additional floor space in an
office or telecommunications room. The use of the large PDS box is less expensive, and it can be wall-mounted along the PDS carrier route, making it more convenient to use. In this case, the PDS box shall meet the same standards as the UDB, including being secured with the same type changeable combination padlock. The use of the PDS box to house the intermediate switch must be closely coordinated with the local security personnel as it will require a risk acceptance from the DAA in order to obtain accreditation for the entire system. The PDS design must also be staffed through the Army CTTA for technical review (see Paragraph 5.2.2) prior to installation or procurement of materials.

4.5.4 SIPRNET Café

a. The use of a SIPRNET Café is ideal for a group of users that only require occasional SIPRNET access. In this type of layout, all of the equipment and PDS is in one room, the café. The storage safe(s) for the computer equipment and other classified material are also typically placed in the SIPRNET Café room. The type of PDS carrier used depends upon whether the café is an open storage area, a CAA, or an LCA. A SIPRNET café shall not be placed in a UAA. The café layout takes advantage of the fact that although there may be multiple SIPRNET users in a facility, not all of them always use SIPRNET or all at the same time. The SIPRNET access is a shared asset. There are fewer UDBs required, but each one typically contains two network connections.

b. The use of the café concept provides a facility level SIPRNET access capability while reducing the size of the required security zone from that of a distributed PDS system. This reduces the associated risk by reducing the necessary physical security upgrades to the facility and by consolidating the local security procedures to a smaller area.

c. The café room selected must be sized to accommodate the <u>Information Processing</u> <u>System (IPS) container</u> [see <u>Paragraph 4.7.4(b)(2)</u>] used to house the network electronics, the storage safe(s), and the maximum number of users expected to be using the café at any given time. In this example a six-user café has been selected. Thus, the UDBs must be placed around the room with sufficient spacing to allow for six users to sit at desks or tables. Typically, the UDBs are placed in the middle between each pair of desks/tables. The spacing between users must allow sufficient space to work and provide a "buffer zone" between users to prevent inadvertent viewing of another user's work (thus maintaining the "need to know" aspect of access to classified information). Each user shall have an absolute minimum 3 foot wide by 2 foot deep working space allocated (the size of a folding field table); although a 4 foot to 6 foot wide space is highly recommended.

d. From an operational aspect, to use the SIPRNET, users must each leave their office and go to the café. This is not too different from the distributed layout in which users must leave their office to procure their classified computer hardware from the storage safe(s). The difference is that users must remain in the café, away from their desk, all during SIPRNET use.

e. As all of the PDS and safes are in one location, the security zone which must be monitored and checked is much smaller, making it relatively easy to turn the entire area into an LCA or a CAA. As café rooms are often in areas of the facility that is not under constant observation during the duty day, the chosen café room should be a CAA. With all of the classified equipment and material in one room, there is typically less chance for an inadvertent security violation.

4.5.5 Individual COMSEC

a. In this physical architecture, individual SIPRNET users are provided their own individual COMSEC device. This eliminates the need for a PDS as the signal is encrypted (i.e., BLACK) all the way from the SIPRNET PoP to the user's desk. While the cost of the PDS is eliminated, it is often more than offset by the cost of the individual COMSEC devices. The breakeven point depends upon the cost of the individual COMSEC device used, as well as the complexity and size of the PDS that would be required, especially in a distributed architecture. However, as a general principle, the breakeven point is typically four users for the SECNET-54 and seven users for the Talon.

b. With individual COMSEC devices, each user's office is a security zone in and of itself whenever SIPRNET is being used in that office. Each office should be at least an LCA, preferably a CAA. Also, measures must be taken to prevent the inadvertent viewing of classified material. The user's SIPRNET computer screen must be oriented such that it cannot be viewed from outside of the office or from the office door. The windows in the room must be covered while SIPRNET is in use in the office to prevent inadvertent viewing of classified material from outside the room. If other personnel besides the user work in the office, they should possess at least a Secret level security clearance.⁴² With multiple separate security zones spread throughout the building in individual offices, the possibility of an accidental security incident occurring increases.

c. When not using SIPRNET, the classified laptop or computer hard drive must be secured in a safe. The COMSEC device must also be stored in the safe or else be rendered unclassified. Rendering it unclassified is normally accomplished by removing the Crypto Ignition Key (CIK), a small round electronic key about 1 inch in diameter and 1/2 inch thick, but the actual process is device dependent. As the COMSEC device remains a Controlled Cryptographic Item (CCI) even when unclassified, it must be properly secured. It must either be secured in a GSA-approved safe or in a locked container inside a locked room. The CIK is also unclassified when removed from the COMSEC device and must be secured in a similar fashion.

d. There are a number of different encryption devices that could be used as individual COMSEC devices, each with different capabilities and unit cost. More details on the capabilities are provided in Paragraph 4.8 and Appendix B.

⁴² AR 380-5, Section 7-20 Paragraph d(1).

4.6 Tunneling

4.6.1 Tunneling is a means of connecting two remote network segments together by using a third network as a means of transport without the transport network being able to read the packets. It is the preferred method of extending SIPRNET access from one building (typically the post SIPRNET PoP) to another (typically a remote tenant facility on post) across the unclassified post CAN. To maintain the confidentiality of the classified information on the SIPRNET, the traffic is encrypted using INEs before transport across the CAN.

4.6.2 As SIPRNET is a C2 network, it has higher standards for the network availability and information security than other networks, such as NIPRNET. Tunneling SIPRNET across the NIPRNET WAN mixes the encrypted SIPRNET traffic in with the NIPRNET traffic, so any network congestion on the NIPRNET adversely affects the SIPRNET traffic. For this reason DISA, from the perspective of the WAN (i.e., the worldwide SIPRNET and NIPRNET), does not allow tunneling of SIPRNET traffic across the NIPRNET WAN. However, this prohibition does not apply to the post unclassified CAN, making tunneling across the CAN a viable solution for extending SIPRNET access a post.

4.6.3 When tunneling across the CAN, it is incumbent upon the local communications provider, such as the NEC, to ensure the transport network (the CAN) carrying the SIPRNET traffic maintains the highest network reliability and availability as possible to reduce potential outages for the C2 traffic on SIPRNET. For CANs that have already completed the I3MP process and are equipped with redundant links and equipment, this does not pose a problem. For CANs that have yet to complete the I3MP upgrade process, a separate means of transport may need to be used.

4.6.4 On an IP-based network such as the post CAN, the IP packets of data occasionally collide, resulting in either the loss of the data or the need to retransmit it, depending upon the protocol being followed by the computer application sending the data. To greatly reduce the possibility of such a collision delaying or destroying a packet of SIPRNET data, the encrypted SIPRNET traffic should be placed in a separate virtual local area network (VLAN) from all other network traffic on the CAN. Although it physically traverses the same cables as the rest of the CAN traffic, the SIPRNET traffic is logically separated from it by the network routers and switches. The SIPRNET VLAN traffic should also be given priority over other traffic at common processing locations, such as routers and switches, to further reduce the possibility of dropped packets.

4.6.5 To utilize VLANs on the CAN infrastructure, each router and switch in the CAN needs to be configured for VLANs. The switch ports on the switches closest to the INEs in each building, typically the EUB switches, are configured for VLAN access while all of the intermediate equipment is configured for VLAN trunking. Only equipment connected to a SIPRNET VLAN port, such as the INEs in various buildings, will receive the IP packets sent on the VLAN.

4.7 Installation of PDS

4.7.1 General

a. The PDS is comprised of three basic components that make up the entire system; the <u>Building PoP</u>, the <u>PDS carrier</u> (conduit, duct or raceway) itself, and the <u>UDBs</u>. Each

component must be properly selected and installed for a PDS to provide the requisite security for the classified cabling inside.

b. Only RED (i.e., unencrypted classified) SIPRNET cabling shall be installed inside the PDS carrier. When using copper cabling, all network cables inside the PDS carrier shall have a red cable sheath. When using fiber optic cabling, the standard fiber optic cabling sheath colors (yellow for single mode and orange for multimode) shall be used.

c. For PDS carriers not secured using welding or compression fittings, a 2-part self-hardening epoxy shall be used to secure all joints and seams, equivalent to the 3M DP-420 series, with at least a 15 minute working life. Clear epoxy, which discolors to a pale yellow upon hardening, should be used as the default for Holocom PDS carrier. Local security personnel may specify the color of epoxy. Epoxy that remains completely clear upon hardening shall not be used.

d. A <u>PDS carrier</u> is a special type of conduit and must be installed as such. The conduit installation guidance provided in the *National Electrical Code* (NFPA 70) is not sufficient. For the installation of PDS, this document and other pertinent communications policies and regulations, most notably NSTISSI 7003, shall take precedence. In all other instances, such as the installation of conduits housing AC power, the policies and guidance in the *National Electrical Code* must take precedence. The PDS shall be installed by properly trained and equipped installation personnel.

4.7.2 Marking and Routing of PDS

a. The RED cables installed in a PDS for SIPRNET access are classified Secret. The PDS acts as a security container for the classified cables. Although the PDS thus effectively stores classified information, it shall not have any external markings that reveal the level of classification of the information stored inside.⁴³ A revised NSTISSI 7003, currently in draft form and not available for publication, will require the PDS to be marked in order to highlight it for ease of visual inspection.

b. The PDS carrier, which contains the classified cabling, shall be installed a minimum of 5 centimeters (cm) (2 inches) away from all parallel BLACK wire lines and AC power lines. If the PDS is parallel with any BLACK wire line or AC power line for 30 meters (100 feet) or more cumulative distance, the separation shall be increased to 15 cm

⁴³ AR 380-5, Chapter 7 Paragraph 7-8.a, Page 81.

(6 inches).⁴⁴ To ensure compliance, the PDS carrier should be installed with a minimum separation of 15 cm whenever possible.

c. If the PDS must cross a BLACK wire line or AC power line, it shall do so at right angles and shall not touch the BLACK wire line or AC power line. It shall be at least 1.25 cm (1/2 inch) away from the BLACK wire line or AC power line where it crosses at right angles.

d. PDS carrier shall be routed and installed such that it does not cross or block access to any window, door, air conditioning duct, or utility opening in the walls, floor, or ceiling of any room or hallway.

e. PDS carrier shall not be routed through public areas where personnel could linger without much scrutiny or that have an expectation of privacy, such as rest rooms or break/lunch areas.

4.7.3 Building -- PoP

a. The network equipment installed for the Building PoP varies widely depending upon the actual site conditions and requirements. One of the simplest consists of a network encryption device (the COMSEC) and a distribution switch. A more complicated one may consist of circuit conditioning equipment, router, firewall(s), network intrusion detection system (NIDS), network intrusion prevention system (NIPS), and a distribution switch.

b. In most cases, given the critical nature of the service provided by the Building PoP to multiple users in the building, a UPS is also included as part of the Building PoP. Regardless of the type and quantity of network equipment used, the network equipment and the security housing for it are referred to as the Building PoP. If a UPS is not already part of the Building PoP, either as a building/facility critical load UPS or as a dedicated UPS in the Building PoP Security Housing, then a UPS should be added to the Building PoP as part of the SIPRNET installation project.

4.7.4 Building PoP Security Housing

a. General.

(1) The security housing for the network equipment is a critical piece of the overall PDS. The security housing is the barrier that prevents unauthorized personnel from accessing the equipment that comprises the PoP. It may be an equipment cabinet, a GSA-approved safe, a dedicated telecommunication room, or even an entire building.

⁴⁴ NSTISSAM 2-95, Paragraph 4.5.1 and Recommendations A thru I.

(2) There are several key factors that must be considered in the selection of the PoP security housing. These factors are discussed in the following paragraphs.

b. Location.

(1) In an open storage area at the Secret (or higher) level, classified material may be stored openly (i.e., not in a GSA-approved safe), as the room itself is the security container. In this case the network equipment may be stored inside a standard equipment cabinet. The equipment cabinet shall be four-sided with a top. The equipment cabinet shall also have keyed locks on each access door to prevent casual access to the equipment inside. An IPS container may be used if additional security is desired.

(2) In areas less than open storage at the Secret level, the network equipment shall be housed in an IPS container. The IPS container is basically an equipment cabinet that is also a security container, or safe, for classified equipment. It is a GSA-approved Class 5 safe that has openings for signal and power cabling and for ventilation/cooling. IPS containers are typically manufactured by the same companies that manufacture standard classified document storage safes. In some cases, an intermediate switch, between the building PoP and a group of distant users, may be needed. This is discussed in more detail in Paragraph 4.5.3.e.

(3) Classified material and off-line classified computer hardware (laptops and removable hard drives) are not permitted to be stored inside an IPS container. These items must be stored in a separate GSA-approved Class 5 or Class 6 safe.⁴⁵ Although the NSA regulation governing the use of IPS containers (CNSSP 10) is in the process of being superseded (by CNSSI 4005), the policy governing storage of classified off-line equipment computer hardware and documents will not be changed.⁴⁶

c. Floor Loading.

(1) The total weight of the PoP is the network equipment plus the security housing. For an equipment cabinet, this can be in the 300-500 pound (lb) range. For an IPS container, it can be in the 1,000-2,000 lb range.

(2) The total weight of the PoP, divided by the total footprint area of the housing, indicates the floor pressure the PoP exerts on the building structure. This is normally expressed in pounds per square foot (lbs/sq ft). Although equipment cabinets are not normally a problem in the area of floor loading, it should still be considered.

⁴⁶ E-mail, NSA CISSP, Mr. Zundel, 27 May 2010.

⁴⁵ CNSSP 10, Section 1 Paragraphs 2.b and 2.c.

(3) When using an IPS container, floor loading shall be considered. To ascertain if floor loading will be a problem or not, determine the total weight of the PoP and security housing footprint, and give that information to the building structural engineer for analysis. For floor loadings exceeding 250 lbs/sq ft, a metal spreader plate under the IPS container may be required to distribute the floor load to acceptable levels. All such determinations shall be made by the appropriate structural engineering authority.

d. Room Accessibility.

(1) The security housing, whether an equipment cabinet or an IPS container, is a large bulky item of equipment that must be able to fit through the doorways, stairways, and hallways throughout the building for delivery into the selected area.

(2) The most common problems occur when using an IPS container, as they are extremely bulky and heavy, making them difficult to maneuver through tight spaces. Depending upon the location of the room chosen, special equipment may be required to deliver the IPS container. The size and weight of this equipment must also be considered when determining if the IPS container can be placed in a room.

(3) It is highly recommended the room selected for the security housing have a minimum of a 32-inch main entrance door. All hallways along the delivery route should be at least 5 feet wide. All other doorways along the delivery route should be larger than the room entrance if possible, but never smaller.

e. Rack Space.

(1) Sufficient rack space for all equipment must be available inside the security housing. Standard rack spaces are available in 19 and 23 inch widths, with 19 inches being the most common in network equipment. Rack space is normally expressed in terms of rack units (RUs).

(2) The height of the security housing shall contain, at a minimum, sufficient rack space for all equipment plus patch panels and cable management equipment, plus space for equipment accessibility as required.

f. Equipment Accessibility.

(1) The security housing shall be deep enough (front to back) to accommodate the longest piece of equipment plus space for cable connectors and bending radius on the front and back of the equipment. Once installed in the security housing, the network equipment must be accessible for initial cabling and connection as well as for any future maintenance or replacement actions required.

(2) For equipment cabinets, this is accomplished through the use of front and back doors on the cabinet. The equipment cabinet shall be located in the room such that both the front and rear door may be opened a minimum of 90 degrees. To prevent casual access to the equipment, the doors must be lockable. The use of standard cabinet locks and hardware is permitted. Removable side panels on the cabinet may be used to supplement, but not replace, the accessibility provided by the front and rear doors.

(3) In an IPS container, the equipment rack inside is either fixed or movable.

(a) Fixed racks are fastened to the sides on the inside of the IPS container. Once the equipment is mounted in the rack, the connections on the rear of the equipment are

only accessible by reaching through the front of the rack and blindly feeling around. When fixed racks are used, extra rack space (RUs) must be allocated to allow for this. At least 3 RUs shall be available below or above each 4 RUs of equipment. These cabling spaces shall be left empty of equipment or blank panels to allow accessibility and to promote air circulation.

(b) Movable racks are those where the entire rack assembly slides or rolls out from inside the IPS container on some sort of track mechanism. This allows access to all sides of the equipment. When this type of rack is used, the movable rack shall extend far enough out from the front of the IPS container to provide a minimum of 6 inches of clearance. A cable control system shall be provided to prevent cables that drape from the back of the movable rack to the back of the IPS container (such as AC power and user drop cables) from falling to the bottom of the IPS container and being pinched or damaged by the rack as it is secured back inside the IPS container, without causing undue stress or stretching of the cables. Details of some IPS containers with movable racks are provided in <u>Appendix J</u>.

g. Ventilation.

(1) The waste heat generated by the network equipment inside the security housing will cause the interior air temperature to rise to dangerous levels and the network equipment to fail if there is not sufficient ventilation to dissipate it. Active cooling measures (i.e., interior air conditioning) are not permitted due to the dire consequences of its failure. Passive heat exchangers are permitted in combination with fans. The room or space where the security housing is located shall have sufficient cooling and ventilation to keep the air temperature at 75° Fahrenheit (F) or lower.

(2) Equipment cabinets shall have ventilation ports on the sides (at top and bottom) and/or the front and rear. In addition, exhaust fans shall be installed to draw hot air out of the cabinet from the top through the top ventilation ports. The top vents, whether in the top of the cabinet or the top of the cabinet sides, shall contain the exhaust fans. Top vents that allow air to enter the top of the rack and immediately exhaust out of the top of the rack through the fans are not permitted. The fans shall be sized to provide sufficient air flow based on the heat load of the equipment and the air temperature in the surrounding room to keep the air temperature inside the cabinet no more than $15^{\circ}F$ above the room temperature.

(3) An IPS container shall be provided with a similar ventilation system. Air vents may be located on the sides or the bottom, but not on the front, rear, or top. The fans shall be sized to provide sufficient air flow based on the heat load of the equipment and the air temperature in the surrounding room to keep the air temperature inside the cabinet no more than 15° F above the room temperature. The exhaust fan shall exhaust air from the upper portion of the IPS container. The air intake may be located on the bottom of the IPS container, the side opposite the exhaust vent, or the bottom of the same side as the exhaust vent.

(4) The security housing, whether cabinet or IPS container, must be located in the room to allow sufficient clearance around all ventilation ports for proper air flow. At least 4 inches of clearance shall be maintained between all vents and any obstructions (such as walls, filing cabinets, storage boxes, other cabinets, etc.).

(5) The top 2 RUs in the rack space in the IPS container and the top 4 RUs in an equipment cabinet must remain empty or only contain passive equipment such as patch panels to help prevent overheating of equipment. The bottom of any rack shelves used inside the rack space shall be vented rather than solid so that air flow is not restricted.

(6) All air intakes shall be filtered to prevent dust and dirt from being drawn into the security housing. The filter shall be easily removable for cleaning and/or replacement.

h. Noise Suppression.

(1) The noise generated by the ventilation system must be accounted for, especially in an office working environment. When the security housing is located in the same area where personnel will be working, such as in a SIPRNET café, the fan and equipment noise from the security housing shall be attenuated down to the level of ordinary conversation (60 decibel (dB) A-weighted) or less.

(2) When located in a telecommunications room or other unattended area, noise suppression is optional.

i. Exterior Cabling Entrance.

(1) The network equipment requires three types of cabling that exit/enter the security housing; AC power, incoming signal to the BLACK side of the COMSEC device, and the RED user drop cables for network access.

(2) The security housing shall have two separate openings for cable entrances, one for BLACK cables (AC power and incoming BLACK signal) and one for RED cables (user drop cables to the UDBs).

(3) For an equipment cabinet used as the security housing, the BLACK cables shall be protected where they enter the cabinet to prevent cable damage from the edges of the cabinet. The carrier for the RED cables shall be continuous from the UDBs into the equipment cabinet to shield the cables from view. The carrier shall enter directly into the cabinet, or the proper type of fitting be used, to provide the same level of protection to the RED cables.

(4) For an IPS container used as the security housing, the RED cable entrance shall be equipped with a heavy duty lockable box covering it to allow the termination of the PDS duct without exposing any of the RED cabling as it is routed from the PDS carrier into the . This RED cable entrance box shall meet the same physical security requirements as the UDBs.

4.7.5 PDS Carrier

a. All PDS conduit, duct, or raceway (generically referred to as "PDS carrier") shall be installed level and plumb along its entire length.

b. The PDS carrier shall be installed using spacers or other standoff mounting hardware to hold it at least 1/2 inch away from the mounting surface to allow for visual inspection of all sides of the PDS carrier. A standoff distance of 1 inch is preferred.

c. When using a PDS carrier with a removable top along its length, a fill ratio of 70 percent should not be exceeded. A fill ratio of 80 percent shall not be exceeded. For PDS carrier that is of solid construction, such as EMT conduit, a fill ratio of 50 percent should not be exceeded, and a fill ratio of 60 percent shall not be exceeded. For solid construction PDS

carrier, a pull string shall be installed in the PDS carrier and be replaced each time cable is pulled through it so that a pull string always remains in place.

d. For solid construction PDS carrier, a pull box shall be installed at least every 180° of bend or change in direction. Pull and junction boxes shall be constructed to the same standards as the <u>UDBs</u>. Pull and junction boxes may be mounted flat against the mounting surface.

e. PDS carrier shall be securely fastened to the mounting surface at least every 5 feet of length and within 18 inches of each end of each piece of carrier.

f. The PDS carrier shall be mounted with a minimum of 4 inches of clearance between the top of the carrier and the ceiling to allow for proper sealing of the PDS. A clearance of 8 inches is highly recommended. PDS carrier should not be mounted to or suspended from the ceiling. The PDS carrier is not permitted to be mounted to, fastened to, or supported by suspended ceiling hardware.

4.7.6 User Drop Boxes (UDBs)

a. All UDBs shall be constructed from a minimum of 16-gauge steel and be of welded construction. They shall be a minimum of 6 inches wide by 6 inches high by 4 inches deep. All boxes (pull, drop, junction, etc.) shall be sized to accommodate the maximum number of cables and PDS carrier connections planned to be placed in/through the box.

b. Hinges for the access door shall be non-removable when the door is closed. Hinge leaves shall be welded to the box and door.

c. The UDB shall be equipped with a locking hasp to secure the access door in the closed position using a changeable combination padlock built to Federal Specification FF-P-2740A with Amendment 1. The Sargent & Greenleaf model 8077 is the only lock that currently meets this specification.⁴⁷ Holocom pull and junction boxes equipped with properly installed internal locking mechanisms to secure the access door are not required to have locking hasps.

d. UDBs shall be mounted between 36 inches and 66 inches above the finished floor, measured to the bottom of the UDB. If modular furniture and/or partitions are to be used in the room, the UDBs should be mounted above the level of the furniture and partitions. The UDBs shall be visible at all times after the furniture and/or partitions are installed.

⁴⁷ E-mail, GSA, Mr. Pollock, 4 May 2010.

e. Drop, pull, junction, and any other type of box or housing containing pre-punched knockouts are not authorized for use in a PDS.⁴⁸

f. UDBs shall be capable of having a standard single or double gang telecommunications cover plate installed inside the UDB for termination of the cables in standard access jacks. The cover plate shall be sufficiently recessed such that it does not interfere with the properly closing and locking of the access door when no user cables are connected to the front of the network access jacks in the cover plate.

4.7.7 Post-Installation PDS Inspection

a. To help ensure that the PDS will successfully pass the accreditation process, it should be inspected after installation to ensure it meets all applicable installation guidance and regulations. A sample PDS inspection checklist has been provided in <u>Appendix C</u> to assist in this process. This checklist should be modified as necessary to accommodate the specific installation project. The inspection should be done in a minimum of two parts.

b. The first part of the inspection, which encompasses the majority of the inspection items, should be performed prior to the application of the epoxy used to seal the PDS. This will allow the inspector to check inside junction and pull boxes as needed. It also allows the inspector to check for the proper installation of locking removable top cap duct to ensure the locking mechanisms are properly installed and functioning.

c. The second part of the inspection should be done after the sealing epoxy has been applied. Its main purpose is to ensure the epoxy has been properly applied. This part of the inspection is also the ideal time to check for finishing work, such as appearance of the PDS and the work site.

d. Additional inspections, such as after the PDS carrier is installed but before cabling is installed, are highly recommended.

4.8 Encryption Devices

4.8.1 General

a. Encryption devices scramble the incoming classified (RED) data using an electronic key that must be loaded into the device, along with a software algorithm hard-coded into the device, to produce an outgoing unclassified (BLACK) data stream. They also operate in the reverse direction to decrypt the BLACK data stream. The BLACK data stream may be safely transmitted over a communications means without fear of

⁴⁸ NSTISSI 7003, Annex B Paragraph 4.a(1)(c).

compromise. Even if it is intercepted, the BLACK data stream will not reveal classified information. Only encryption devices certified by NSA at Type 1 may be used to transmit classified information over an unclassified transmission media.⁴

Within the U.S. Army, all COMSEC devices must be obtained through CSLA.⁵⁰ b. CSLA has established the Information Systems Security Program (ISSP) for this purpose. Orders for COMSEC devices must be validated through the ISSP website.

https://issp.army.mil (Requires AKO login to ISSP website.)

The key loaded into the encryption device and used to scramble the data is referred c. to the "keying material," or "keymat" for short. Keymat must be obtained thru the proper COMSEC channels. It is normally provided by the NSA through its Electronic Key Management System (EKMS). Keymat is classified to the highest level of classified information that it may be used to encrypt. A Secret level keymat may be used to encrypt Secret or below information but not Top Secret or above. The keymat is downloaded from NSA into a key loading device for temporary storage until it is later downloaded into the COMSEC device for actual use. There are currently two key loading devices in use, the CYZ-10 DTD and the PYQ-10 SKL.

The encryption devices as well as the key loading devices operate using a CIK. d. The keymat does not reside on the CIK. Rather, the CIK merely "unlocks" the encryption or key loading device and allows it to operate. Regardless of the level of keymat contained in a device, when the device and the CIK are separated, both are unclassified unless noted otherwise. Although unclassified when the CIK is removed, the encryption devices and key loaders remain CCIs and must be accounted for and protected against actions that could affect its continued integrity.⁵¹

The only piece of the device that remains classified when separated from the other e. pieces is the Field Tamper Recover (FTR) CIK. The FTR CIK is a special CIK that can be used to recover an encryption device after it has ceased operating due to tampering. The FTR CIK is classified Secret and must be accounted for and protected accordingly.

The keymat used may be one of two types; Pre-Placed Key (PPK) or Firefly Vector f. Set (FVS), more commonly referred to as "Firefly." PPK is similar to that used in much older devices in the exact same keymat must be used on each end of an encrypted

 ⁴⁹ AR 25-2, Chapter 6 Paragraph 6-1.a(1), Page 52.
⁵⁰ AR 25-2, Chapter 6 Paragraph 6-1.a(4), Page 52.

⁵¹ TB 380-41, Chapter 5 Paragraph 5.2.7.a.

communications channel. Firefly is different in that each end of an encrypted communications channel must use a different Firefly key. Firefly works in a fashion similar to the Public Key Encryption (PKE) scheme used to encrypt e-mail messages between two different users. The Firefly key exchanges digital signatures with the remote end during the "handshake," or synchronization process, to valid the communication channel and develop the actual Transmission Encryption Key (TEK). Typically, the crypto period, or length of time for which the keymat is valid, is one month for PPK and one year for Firefly. So that new keymat does not have to be loaded into a COMSEC device every month, modern COMSEC devices can typically store up to year's worth of PPK.

g. PPK is designed for point-to-point communication channels while Firefly is designed for point-to-multipoint communications. Both may be successfully used on data networks. While both PPK and Firefly may be loaded into a COMSEC device at the same time, the two are not interoperable with each other. An encrypted communication channel or link must use PPK or Firefly at both ends. Modern COMSEC devices are capable of housing both types of keymat at the same time, using PPK for some communication channels and Firefly for others simultaneously.

h. The keymat loaded into an encryption device is not used to actually encrypt the data transmitted. Rather, the COMSEC devices use the keymat to synchronize with each other and develop the TEK, which is used for data encryption. This TEK is automatically changed every 24 hours during the active crypto period of the keymat. For this reason it is important that every COMSEC device used in a system be set to the same time and time zone, with a maximum time variation between all devices of 10 minutes.

4.8.2 Types of Encryption Devices

a. General.

(1) There is a wide variety of encryption devices designed for use with different transmission methods. Generically, devices used to encrypt and decrypt information are referred to as COMSEC or encryption devices.

(2) When used to encrypt National Security Information (NSI), the COMSEC devices must be certified by the NSA for Type 1 encryption. 52

(3) There are three basic groups or types of encryption devices, discussed in the following paragraphs. Some COMSEC devices are capable of operating in more than one of

⁵² AR 25-2, Chapter 6 Paragraph 6-1.a, Page 52.

these configurations. Specifics on the various models of encryption devices and its availability are provided in <u>Appendix B</u>.

b. Link Encryptors.

(1) Link encryptors are those devices that are members of the Link Encryption Family (LEF). They are designed for used on link and trunk circuits typically found in long-haul transmission. They are usually designed for serial circuits such T1s, Digital Signal Level 3s (DS3s), or other high capacity circuits. As these high capacity circuits are often the aggregate of many smaller circuits, they are also referred to as trunk encryptors.

(2) Current link encryptors found in the LEF are the <u>KIV-7M</u>, <u>KIV-19M</u>, <u>KG-75A</u>, and the <u>KG-340</u>.

c. In-line Network Encryptors (INEs).

(1) Encryption devices designed to be used in IP-based data networks in between network devices are generically referred to as INEs. Although INEs have been used since the early 1990s, it is only since 2000 that its use has become widespread. This has resulted in the need for standards for interoperability and IA.

(2) Current INEs typically used for classified networks are the <u>KG-175</u> Tactical Local Area Network Encryptor (TACLANE), <u>KG-240 ViaSat</u>, and <u>KG-250 RedEagle</u> families of INEs. Each family of INEs has several varieties with slightly different network capabilities.

d. Individual Mobile Encryptors (IMEs).

(1) INEs designed for use by a single user rather than a network of users are referred to as IMEs. The <u>KOV-26 (Talon)</u>, <u>KIV-54 (SecNet-54)</u>, and <u>KIV-11 (SecNet 11</u> <u>Plus)</u> are examples of IMEs.

(2) IMEs are particularly useful for personnel who must travel (i.e., are mobile) and need access to SIPRNET while traveling. However, when used in this fashion the physical security of the classified computer hardware and the IME often present sufficient disadvantages to outweigh the advantage of secure mobile computing. They are also useful for the individual COMSEC architecture described in Paragraph 4.5.5.

4.8.3 High Assurance Internet Protocol Encryptor (HAIPE)

a. A HAIPE is an encryption device that was manufactured under the HAIPE Interoperability Specification (HAIPE IS), which is a standard developed to ensure interoperability between various encryption devices regardless of manufacturer. This standard does not detail any performance or environmental requirements. The HAIPE IS used to be known as the High Assurance Internet Protocol Interoperability Standard (HAIPIS).

b. The HAIPE IS has undergone several revisions since the initial publically available specification, Version 1.3.4, was released in October 2003. Version 1.3.5, the first Army adopted standard, was developed in May 2005 as one large document. The first HAIPE IS compliant INEs were developed to this version as a hardware solution. Version 2 was released at the same time, but was not too useful, as Version 3 was developed in March 2005. Beginning with Version 3, the standard was written as several separate documents, a core specification and several extensions, enabling incremental development

and implementation of the specification. Version 3.0.2 was released in December 2006, just days before Version 3.1.0. Version 3.1.2 of the standard was finalized on 29 February 2008. Version 4.0 was finalized on 31 March 2009.

c. It typically takes 18-24 months after the standard is updated before products meeting it are available. Thus, sometime in 2010, products compliant with v3.1.2 will become available, mostly through software upgrade. Currently, any INE purchased after 30 September 2008 must be compliant with HAIPE IS v3 or higher. ⁵³ So the currently available operational HAIPE IS is v3.0.2.

d. Version 3 added support for IPv6 to the specification, a key addition in line with the Army planned migration to IPv6. It also added the capability for over the network management, leading to the development of the various remote management software packages for INEs. The incremental revisions of the HAIPE IS since then have refined these specification extensions and added others. An extension for Over The Air Rekey (OTAR), the ability to transfer keymat from HAIPE to HAIPE across the network link, was added to the standard in HAIPE IS v3.1.2.

e. From the development of products meeting HAIPE IS v1.3.5, upgrades to future versions of the standard have been able to be accomplished by software upgrades in the field. All INEs currently authorized for use have manufacturer upgrades to v3.0.2 available. Manufacturers are currently working on upgrades to v3.1.2.

f. Additional information regarding the HAIPE IS can be obtained from the Information Assurance Support Environment (IASE) website.

https://powhatan.iiie.disa.mil/haipe

4.8.4 Remote Management

a. Part of the HAIPE IS v3 is the ability to remotely monitor, manage, operate, and configure multiple COMSEC devices from a centralized location. This provides for a centralized policy on the management of many devices spread over a large geographical area. The result is a labor cost savings as managing a large number of devices thus requires fewer personnel and no travel time/costs to the sites of the COMSEC devices. The protocol used for remote management is Simple Network Management Protocol version 3 (SNMPv3).

⁵³ CNSSP 19, Section IV Paragraph 8.

b. Although the HAIPE IS was developed for interoperability and it specifies a common management information base (MIB) for remote management, the remote management software used to manage HAIPE devices is proprietary to the manufacturer of the device. Each manufacturer has developed a software package that remotely manages its family of devices.

(1) For the KG-175 TACLANE family of INEs, manufactured by General Dynamics, C4 Systems division, the GEM X software package is available for remote management. It will manage up to 500 TACLANE and FASTLANE devices on a Windows or Sun-based computer platform. There is also a smaller version, GEM X Lite, for up to 25 devices, that is provided with each TACLANE purchase at no cost. An upgrade program from a previous version, GEM, is available. Additional information is available on the General Dynamics C4 Systems website.

http://www.gdc4s.com/content/detail.cfm?item=45b9abed-a178-486e-908b-28f858754155

(2) For the KG-240 RedEagle family of INEs, manufactured by L-3 Communications, the remote management software package is its Common HAIPE Manager. It will manage up to 10,000 devices from a Windows or LINUX-based computer system. Additional information is available on the L-3 Communications website.

http://www.l-3com.com/CS-East/ia/redeagle/ie_ia_redeagle.shtml

(3) For the KG-250 AltaSec family of INEs, manufactured by ViaSat, the VINE Manager software package is available. It will manage 250 to 2,000 AltaSec INE devices on a Windows-based computer platform, based on the platform and the Windows operating system (OS). It is available free for users of the AltaSec INEs. Additional information is available on the ViaSat website.

http://www.viasat.com/government-communications/information-assurance/viasatine-manager-software-vine

(4) For the KIV-7MiP INE, manufactured by SafeNet, Inc., the SafeEnterprise Security Management Center software is available. It will manage any number of SafeNet HAIPE devices on a Sun Solaris-based computer platform. Additional information is available on the SafeNet website.

<u>http://www.safenet-</u> inc.com/Products/Data_Protection/Network_and_WAN_Encryption/Commercial_ Encryption/Security_Management_Center.aspx

c. There is no interoperability specification or standard such as the HAIPE IS for link encryption devices, so there is typically no software package available for remote management of these devices. IMEs are a sub-family of INEs and must follow the same requirements for compliance with the HAIPE IS.

4.8.5 Support, Training, and Maintenance

a. Technical support for the COMSEC devices and the remote management software is available from all of the manufacturers. Initial source of support should be the manufacturer's website. b. Operator training for the COMSEC devices and remote management software is also available from all of the manufacturers. Training is done either at a manufacturer facility or at the customer location. There is a cost to the training programs regardless of which location is used. However, it is usually much more cost effective to house it at a local facility if several students are to be trained at the same time.

c. Maintenance support is normally provided through warranty and extended support. The warranty on COMSEC devices varies but is normally a 3- or 5-year warranty on hardware and software. Additional annual maintenance may be purchased for after the warranty expires. Maintenance on the remote management software, in the form of software upgrades, is available for purchase. Up to date information is available on each manufacturer's website.

4.9 Secure Wireless Local Area Networks (SWLANs)

4.9.1 General

a. WLANs use a radio link to transmit and receive information between two wired LANs (referred to as Bridge mode) or between a wired LAN and an end user (referred to as Access mode). The standard used for wireless networking is the Institute of Electrical and Electronics Engineers (IEEE) 802.11 series of standards. This document will only be concerned with WLANs (802.11a/b/g/n) and not with other wireless technologies such as wireless personal area networking (802.15, or Bluetooth) and Worldwide Interoperability for Microwave Access (802.16, or WiMAX), pagers, cellular telephones, etc..

b. DOD's policy is that unclassified WLAN systems must be standards-based and IEEE 802.11 compliant. In addition, to help protect the information in the transmitted radio signal, the system must use Wireless Protected Access 2 (WPA2) enabled devices that implement the Advanced Encryption Standard (AES).⁵⁴ This helps protect the WLAN from unauthorized access at the link layer.

c. Equipment used in classified WLANs must be certified by the NSA and the WLAN must use NSA Type 1 encryption devices, as well as be protected by physical security measures appropriate for the classification of the NSI being processed.⁵⁵

4.9.2 Wireless TEMPEST Issues

a. As the transmission link is a radio signal, any receiver, whether authorized or not, that is within range of the signal can capture it. The radio signals penetrate most building

⁵⁴ DODI 8420.01, Enclosure 3 Paragraph 1.a.

⁵⁵ DODI 8420.01, Enclosure 3 Paragraph 4.a and 4.b.

materials, so the unauthorized receiver does not necessarily need to be in the same facility. TEMPEST is the name given to the evaluation and control of the compromising emanations from telecommunications and automated information system (IS) equipment. To prevent unauthorized persons from receiving, reading, and exploiting the information transmitted, special security measures must be taken when implementing WLANs. These special measures are generally known as TEMPEST countermeasures, an unclassified codename referring to the measures taken to contain the compromising electromagnetic emanations within the controlled inspectable space around the equipment or facility.

b. NonStop is an unclassified codename for some highly classified TEMPEST issues. Due to these TEMPEST issues, the use of wireless communications devices, such as twoway radios, pages, Bluetooth devices, etc., will be prohibited from areas where classified information is discussed or processed, such as SIPRNET rooms.⁵⁶ These devices may be permitted if certain conditions are met⁵⁷ and are approved by the DAA after a technical review by the Army CTTA. Additional and more detailed information regarding TEMPEST issues may be obtained from the Army CTTA.⁵⁸

c. The location of any fixed RF transmitting device or antenna within 10 meters of fixed RED processing equipment in a SIPRNET area is of special concern in the area of TEMPEST.⁵⁹ A fixed RF device or antenna is one that remains in a specific location and orientation for an extended period of time. A laptop computer that is placed on a desk at the beginning of each day and removed at the end of each day is not considered fixed. If the laptop is placed on the desk and not moved each day, or is placed in a docking station that is left in the same position on the desk every day, it is considered to be fixed.

4.9.3 SWLAN Design Considerations

a. A SWLAN provides a solution to providing SIPRNET access services that may reduce the time and manpower required to setup and operate a secure communication infrastructure. Although wireless solutions may have merit in certain situations and applications, wireless SIPRNET may not be the best choice for the "normal" SIPRNET user. The minimum separation distance limitations as set forth in national and Army policy⁶⁰ may limit the number of secure wireless devices that can be installed in an area.

⁵⁶ AR 25-2, Paragraph 4-29.a, Page 46.

⁵⁷ Unsigned Memorandum, IAMG-CIC-OP-CTTA, Paragraph 3.

⁵⁸ CTTA TEMPEST Information Handout.

⁵⁹ AR 380-27, Chapter 4, Paragraph 4-1.

⁶⁰ NSTISSAM 2-95, NSTISSAM 2-95A, and Memorandum, IAMG-CIC-OP-CTTA.

b. To provide SIPRNET access via a SWLAN, the SWLAN is used to extend the service from the wired portion of the local SIPRNET infrastructure. The connection of the SWLAN to the wired portion of the local SIPRNET must be part of the SWLAN design. This part of the SWLAN must be implemented following the criteria in other sections of this document.

c. As shown in <u>Figure A-8</u>, three basic architectures are approved for use in SWLANs.⁶¹ An actual SWLAN may also be a combination of the different architectures.

(1) The Wireless Access architecture is the one most commonly thought of. This is when the WAP is operated in Client Access mode, allowing users to connect to it via the wireless connection while the wired side of the WAP is connected to the network. It is used to grant wireless users access to a wired network.

(2) The Wireless Bridging architecture is when two or more WAPs are operated in Bridge mode. This architecture is used to extend a wired network from one location to another via the wireless connection between the WAPs. Operated in this mode, the WAPs normally will not allow wireless clients to connect to them.

(3) The Peer-to-Peer architecture is an "ad-hoc" network that is setup between local clients via its wireless capabilities. It does not require a WAP as all connections are between the clients. This type of wireless architecture is not recommended, as by directly linking the clients all network security and monitoring devices are bypassed, allowing a virus or Trojan horse program on one client to easily spread to the others.

d. While setting up a SWLAN appears simple, and from a wireless client perspective it is, there are a number of management burdens associated with SWLANs that increase the operations and maintenance (O&M) burden of operating a SWLAN. Each requires the expenditure of equipment or manpower resources beyond the actual wireless client connection.

(1) A wireless intrusion detection system (WIDS) must be employed throughout the entire area of operations (not just the area where authorized WLANs are used) to monitor for unauthorized WLAN usage, whether secure or non-secure.⁶² The WIDS must monitor all WLAN frequency bands available, not just those used locally for wireless access or bridging. For a large area, such as the metropolitan area size of most cantonment areas on Army posts, this can represent a large number of devices.

⁶¹ DISA Wireless STIG, Paragraph 3.2.4.

⁶² DISA Wireless STIG, General Wireless Policy, Page 1, Vulnerability Key V0018596.

(2) A WIDS server must be employed to continuously monitor the deployed WIDS.⁶³ This requires personnel to periodically review the server logs for signs of unauthorized WLAN activity and take the appropriate action.

(3) Only authorized wireless systems may be employed in a WLAN.⁶⁴ For a SWLAN, only devices with NSA Type 1 encryption may be used.⁶⁵ The only devices currently authorized for use in a SWLAN are the SecNet 11 Plus (KIV-11), the SecNet 54 (KIV-54) and the Talon (KOV-26).⁶⁶ Technical details of these COMSEC devices are available in <u>Appendix B</u>. Due to its proprietary implementation of the 802.11 standards, the SecNet 11 Plus is not recommended for use in a SWLAN.

(4) The WAPs and other equipment used in a SWLAN must be afforded additional physical security controls above those afforded most wired network connections. If the device is not stored inside an approved security container, such as an IPS container, it must be physically inventoried each day.⁶⁷

(5) A WIDS is a wireless network transmitter just like a WAP. As such, the design and implementation of the WIDS portion of a SWLAN must also be reviewed by the Army CTTA for potential TEMPEST issues prior to the installation and operation of the WIDS equipment. It is highly recommended the review be done prior to the procurement of any equipment, during the design phase of the project.

e. As shown in the paragraphs above, the design and implementation of a SWLAN involves much more than just selecting equipment. It involves the design and implementation of local policies and procedures to ensure all aspects of network security are addressed in order that the system may be accredited and approved for use. All of which involve additional costs that must be factored into the decision between using a wired and a wireless network.

4.10 Voice over Secure Internet Protocol (VoSIP)

4.10.1 General

a. Telephonic communications over an IP-based network have become a quick and easy means to establish voice communications worldwide. As the requirements for

⁶³ DISA Wireless STIG, WLAN IDS Checklist, Page 1, Vulnerability Key V0014887.

⁶⁴ DISA Wireless STIG, General Wireless Policy, Page 3, Vulnerability Key V0008283.

⁶⁵ DISA Wireless STIG, Classified WLAN System Checklist, Page 6, Vulnerability Key V0015300.

⁶⁶ DISA Wireless STIG, Paragraph 3.2.4.

⁶⁷ DISA Wireless STIG, Classified WLAN System Checklist, Page 9, Vulnerability Key V0018584.

SIPRNET access increase, so do the requirements for a secure Voice over Internet Protocol (VoIP) system, referred to as VoSIP. VoIP is a real-time application, meaning the IP data packets containing the voice must be delivered to the distant end in a timely fashion and in sequence. Failure to do so results in the loss of quality in the communication, making the voice received either unrecognizable and/or unintelligible. Steps taken to ensure the quality of service (QoS) of the VoIP link will ensure the timely sequential delivery of the voice packets.

b. VoSIP is merely the use of VoIP in a classified network environment. It affords users the ability to hold classified telephone conversations over their existing classified IP network. For a VoSIP call over the SIPRNET, the conversations may be at the Secret or below level.

c. As in a normal analog telephone call, a VoSIP/VoIP call has two main parts, the call setup and the call conversation. The call setup is not time sensitive like the conversation is, as it uses the Transmission Control Protocol (TCP) portion of the IP standard. The time sensitive nature of the conversation lies in its use of the User Datagram Protocol (UDP) portion of the IP standard, in which the data packets are sent out, relying on the network to get them to its destination in sequence and in a timely fashion. This reliance on UDP is what makes VoIP calls susceptible to lack of QoS. In a dynamic network such as the Internet, the NIPRNET or the SIPRNET, where the VoIP packets are mixed in with all of the other packets, there are inevitably delays and losses resulting in a low quality or even dropped conversation.

d. Although VoSIP will provide secure voice communication that can be used for C2 functions, it will not replace the DRSN. DRSN, with the proper COMSEC device and keymat, can be used for any classification of call. It also provides many other functions that VoSIP cannot, such as preemption. While the DRSN system requires special telephone sets and switching equipment plus extensive setup of the circuits linking them, VoSIP is relatively simple to establish at its most basic level.

4.10.2 Types of Calls

a. IP-to-IP Call.

(1) The IP-to-IP call is the simplest VoSIP call. It is a direct point-to-point call using IP addresses instead of telephone numbers. This is accomplished by hooking a VoIP phone to the SIPRNET at each location, assigning a local IP address to each one, and "dialing" the distant end by entering the distant ends IP address.

(2) There is no QoS involved in this type of call, and it frequently suffers from packet loss, making some conversations difficult to conduct. If there are firewalls included in the local network security equipment on either SIPRNET segment, the call may not be able to establish at all. This type of call should not be relied upon for critical C2 conversations.

b. Dialed Call.

(1) DISA has developed a VoSIP capability as part of the DRSN for those users that do not require the full capabilities of the DRSN, but do need IP-based voice communication. This system provides a global directory service that enables users to dial a telephone number to reach a specific VoSIP phone. In addition, they provide links between

the VoSIP part of the system and the rest of the DRSN. The DISA VoSIP implementation also provides the ability for a VoSIP phone on SIPRNET to communicate with a secure phone, such as a STE that is connected to the Public Switched Telephone Network (PSTN), via the DRSN. At this time, the system only provides QoS at the local enclave (i.e., on post). Although the global WAN portion is highly reliable, full QoS has not yet been implemented.

(2) Similar to regular analog telephone service, DISA provides three classes of service for VoIP/VoSIP.⁶⁸ Class A service requires proper justification.

- Class A: Worldwide IP-to-IP access plus IP-to-DRSN access
- Class B: Worldwide IP-to-IP access
- Class C: Local enclave IP-to-IP (i.e., on post) access

(3) The call director equipment in the DISA system translates between the IP addresses and telephone numbers, similar to the way Domain Name Services (DNS) translates between the web page Uniform Resource Locator (URL) and the server IP address when browsing the Internet. The telephone numbers used must be taken from the global numbering plan used by DISA.⁶⁹

(4) Under the global numbering plan, DISA assigns the area code and the Network Numbering Exchange (NNX) part of the 10-digit telephone number (ex: 304-NNX-XXXX). The last four digits are assigned by the local VoSIP enclave administrator (typically the NEC). The dialing format within an area code will be 7-digit, with 10-digit dialing between area codes and when dialing from VoSIP-to-DRSN. Dialing from DRSN–to-VoSIP will use a 12-digit dialing format, the same 10-digit format as for other calls, but prefixed with a "80" redirect number code. The area codes used in the DISA numbering plan are shown in Table 1.

⁶⁸ DISA DRSN-VoSIP Connection Guide, Paragraph 4.4, Page 6.
⁶⁹ DISA DRSN-VoSIP Connection Guide, Paragraph 4.3, Page 5.

⁵⁰

Location	Area Code	Location	Area Code
CONUS	302	Africa	301
CONUS Tactical	702	Pacific	305
CONUS Special User	201	SWA (CENTCOM)	308
Europe	302	SWA Tactical (Iraq)	708
Europe Tactical	704	SWA Tactical	718
		(Afghanistan)	

Table 1. VoSIP Area Codes

CENTCOM=Central Command; SWA=South West Asia

(5) Likewise, the IP addresses used for the VoSIP equipment must be taken from an IP subnet issued by DISA specifically for VoSIP use⁷⁰. Use of local IP addresses on the global VoSIP network is not authorized as they will not provide the desired connectivity due to network routing issues.

(6) The equipment used within the local VoSIP enclave must be listed on the DISA Approved Products List (APL).⁷¹ The current APL can be found at the following DISA website.

http://jitc.fhu.disa.mil/apl

(7) To implement QoS on the local VoSIP enclave, a separate VLAN must be created for all of the VoSIP traffic and equipment. As the IP addressing used for the VoSIP equipment comes from DISA and will be different from what is normally used locally, placing the VoSIP equipment and traffic in a VLAN separate from all other local traffic is a natural consequence of proper network design and planning. This VoSIP enclave must be afforded the proper network security between the enclave and where it connects to the WAN (in this case, the SIPRNET).⁷² At a minimum, the network security must include an external and internal NIDS, a router with access control lists (ACLs), and a firewall.⁷³ This network security equipment may be dedicated to the VoSIP enclave, or it may be part of a larger enclave's security perimeter, such as a SIPRNET PoP provided by an NEC on post.

⁷⁰ DISA DRSN-VoSIP Connection Guide, Paragraph 4.2, Page 5.

⁷¹ DISA DRSN-VoSIP Connection Guide, Paragraph 3.2, Page 3.

⁷² DISA Enclave STIG, Paragraph 2.9, Page 18.

⁷³ DISA Enclave STIG, Paragraph 2.92., Page 20.

4.10.3 Future of VoSIP

a. Currently, many installations and organizations have implemented a local VoSIP capability, complete with directory services. DISA has implemented a global VoSIP backbone with a global directory service, as discussed in the paragraphs above.

b. The Army Chief Information Officer (CIO)/G6 has formed a working group to make recommendations on the future of VoSIP implementations within the Army. The recommendations will be to create an Enterprise model for VoSIP with centralized management, call processing, and directory services, linked into the DISA VoSIP architecture. Pending the implementation of the Enterprise model, the Army CIO/G6 will be limiting local implementations of VoSIP within CONUS.

c. Additional information on the VoSIP working groups study is available at the AKO website.

https://wiki.kc.us.army.mil/wiki/Army_VoSIP (Requires AKO login to website.)

4.10.4 Secure Voice

a. In the area of secure voice communication, the Secure Communications Interoperability Protocol (SCIP) has been in use since 2001. In 2004 it replaced the Future Narrowband Digital Terminal standard as the Government standard for secure voice communications. It is designed for land line and cellular telephone systems. Such systems are operated separately from SIPRNET and are thus beyond the scope of this document.

b. Some examples of secure voice systems are the STE, Sectera Wireline Terminal (SWT) for land line products and Sectera Global System for Mobile (GSM) and Qsec-2700 for wireless (cellular) products.

4.11 Video Teleconferencing (VTC)

4.11.1 General

a. VTC in a classified environment may be accomplished as either a direct one-to-one link between two suites of VTC equipment or as a bridged link using a gateway bridge device to allow two or more suites of VTC equipment to connect. Typically, the VTC connection is via an Integrated Services Digital Network (ISDN) connection or an IP network.

b. DISA, through its DISN Video Services-Global (DVS-G) network, provides worldwide VTC bridging services. The DVS-G currently is an ISDN-based system. The new generation, DVS-G II, will provide both IP- and ISDN-based bridging services, as well as conversion between the two. The DVS-G II is currently being fielded, and some high-level users and sites have already converted to IP-based VTC systems.

c. Until DVS-G II is fully operational, new users will be able to register their VTC system and use the DISA bridging services in ISDN mode only. New users will be able to register their IP-based VTC systems on DVS-G II after the fielding is completed. Point-to-point IP-based VTCs between two users will always be possible since they do not use the DISA bridging services. However, VTCs that do not use the DVS-G II services will not have a guaranteed QoS, so the video and audio may degrade or be disrupted at inopportune times.

d. Additional information regarding the DVS provided by DISA is available at the DISA website.

http://www.disa.mil/connect/classified/dod_new_dvs.html

4.11.2 Types of VTC Systems

a. A VTC system may be used for unclassified VTCs only, for classified VTCs only, or as a multi-domain system used for both unclassified and classified VTCs. When switching a VTC between domains, sufficient procedures must be followed to prevent a security compromise. Some VTC systems perform such procedures automatically with the flip of a switch while others must be manually re-cabled and reconfigured in a specific sequence.

b. When the VTC system is designed for classified VTCs only, the VTC coder/decoder (CODEC) may be configured with both an Ethernet and V.35/RS-449/RS-530 port. The Ethernet port allows secure IP-based VTCs directly through the SIPRNET, while the V.35/RS-449/RS-530 allows ISDN dial-up connectivity. Figure A-9 depicts a simplified view of a VTC system equipped for both ISDN- and IP-based secure-only operation. To prevent security violations when a secure ISDN VTC is taking place, the IP path must be disconnected. Conversely, when a secure IP VTC is taking place, the ISDN path must be disconnected.

c. When the VTC system is designed only for unclassified VTCs, the main difference from a classified-only system is that the unclassified VTC system does not include an encryption device. The inverse multiplexer (IMUX) serial port is connected directly to the CODEC serial port, and the CODEC IP port is connected directly to the unclassified IP network. Operationally, neither the ISDN nor the IP connection needs to be disconnected when the other is being used.

d. For multi-domain VTC systems, steps must be taken to ensure no information from the classified side is leaked into the unclassified side. This includes CODEC configuration information. When switching from classified to unclassified use, all configuration information must be flushed from the system, and the system must then be reconfigured for unclassified use before being connected to the unclassified network. The CODEC must be disconnected from both domains during this procedure. It is incumbent upon the VTC system owner to ensure these security measures are implemented and followed, through manual and/or automatic procedures.⁷⁴ Figure A-10 shows simplified view of a VTC

⁷⁴ DISA VTC STIG, Paragraph 7.1, Page 89.

system configured for both ISDN- and IP-based secure or non-secure operation. The optical isolators allow only one path, either the secure or the non-secure one, to be active at any given time.

e. The VTC equipment is typically installed in a portable roll-around cabinet with a flat panel display on top for use in conference rooms. Portable systems packed in special cases are also available for deployment use. For fixed applications in conference rooms or auditoriums, the VTC equipment may also be mounted in fixed equipment racks or cabinets. Display devices will vary based on the individual user requirements. Flat panels, fixed projectors, or portable projectors are typically used to display images. When projectors are used, fixed or portable screens can be installed for use in conference rooms. For deployment situations, the small display screen built into the cases can be used for small conferences. Ports are typically available on them to allow the addition of portable displays or projectors and screens to the system for larger venues. Projection screen sizes should be tailored to match the characteristics of the particular VTC room or area and the audience size. Although VTC systems are typically configured with built-in audio capability, a supplemental audio system may need to be added to provide sufficient volume and clarity of sound, depending upon the location and layout of the VTC room.

4.11.3 Design and Use Considerations

a. A secure VTC system must be used in such a manner to prevent the public from viewing or overhearing classified information from the VTC. Keeping the entry door(s) closed and locked (if possible) during VTC operation is the best method to ensure compliance. If windows are present in the secure conference room, the window coverings should be drawn closed to preclude outside viewing of the VTC displays. There should also be sufficient audio attenuation through the walls and doors to prevent a person standing outside the room from understanding what is being said inside the room. The outside listener may be able to discern that someone is talking but should not be able to understand what is said.

b. In addition, measures must be taken to ensure collateral information is not inadvertently transmitted to the other VTC participants. Collateral information is information that is in the VTC room but is not part of the VTC presentation or discussion. Examples of visual collateral information that could be disclosed by the VTC camera are papers lying on a table in front of a VTC participant, posters on a wall in the VTC room, papers left behind by previous meetings held in the room, or a chalkboard off to the side that

is within the cameras view. Examples of audio collateral information are sideline conversations between participants in the same VTC room, a telephone conversation held by someone in the VTC room that is out of view of the camera, or conversations/noise entering the VTC room from outside through doors, windows, or ventilation openings. To prevent the disclosure of collateral information while the VTC room is in use for other than a VTC, power off the VTC system. If it cannot be or is not powered down, then the microphone audio must be muted and the camera must be covered or blocked.⁷⁵

For an IP-based VTC, the VTC equipment must be assigned an IP address from a C. subnet different from normal network users, and it must be operated in a separate VLAN reserved for VTC equipment.⁷⁶

Wireless network connectivity should not be used to connect VTC equipment into d. the network. This is especially true for secure VTCs connecting to the SIPRNET. If wireless connectivity is used, it shall meet all of the criteria and policy for WLANs.⁷⁷ This includes the use of wireless technology for microphones, cameras, data sharing, whiteboarding, speakers, displays, and control panels used as part of the VTC system.

Similar to VoSIP, IP-based VTCs use TCP for the signaling to establish and control e. the VTC and UDP for the actual transmission of the video and audio portion of the VTC. The firewalls used as part of the network security equipment protecting the VTC enclave and/or the local network access to the WAN may block incoming IP-based VTCs if not properly configured. Unfortunately, the IP ports and protocols that could be used by an IPbased VTC cannot all be allowed through the firewall due to the large number of them and the fact that many are used by other, potentially malicious applications as well. Special application-aware firewalls designed for use with VTCs may be used to mitigate this issue. There are also firewall traversal technologies, based on the H.460 standard, that allow incoming and outgoing VTCs through a firewall without having to open large holes in the firewall for the numerous ports and protocols required. Firewall traversal technologies typically use a border controller on the outside of the firewall to receive incoming VTC traffic and a gatekeeper inside the firewall, which coordinate and pass the VTC traffic between them, through the firewall, using a very limited number of specified ports and

⁷⁵ DISA VTC STIG, Paragraph 3.2.2.1 and 3.2.2.2, Page 24.
⁷⁶ DISA VTC STIG, Paragraph 5.1, Page 71.

⁷⁷ DISA VTC STIG, Paragraph 5.1.1, Page 73.

protocols. This solution can be used with almost any firewall, application aware or not. The use of application aware firewalls is the preferred solution.⁷⁸

4.11.4 Secure VTC to the Desktop

a. Secure VTC to the desktop allows users to participate in a secure VTC while sitting at their SIPRNET computer instead of having to relocate to a VTC room. The hardware requirements for a desktop VTC are typically just a camera and a microphone. The software varies in capability, from allowing the user to participate in a one-on-one VTC to allowing the user to host a point-to-multipoint VTC with full collaboration and sharing of applications. Individual user rights on the secure computer and the configuration of the network to allow the required ports, protocols, and services to pass while maintaining network security, must be addressed as well.

b. The complexity and variety of hardware, software, and LANs from site to site make the discussion of secure desktop VTC beyond the scope of this document. However, the same considerations given to securing IP-based deployment systems are warranted and required.

4.12 Thin Client

4.12.1 General

a. This client computing refers to a system that relies on another computer to function. A this client solution has three basic pieces to it, the back-end (sometimes called the head-end), the network, and the user-end (sometimes called the terminal).

b. The workstation provides the end user interface. The network provides the required connectivity. The back-end, or the server location, provides the OS and application software as well as the data storage. The thin client workstation, or terminal, does not have a dedicated hard drive in it that's used for storing data. The size of the OS and productivity software on the terminals is greatly reduced as the bulk of the software resides on the servers at the back-end of the system. Typically, the back-end of the system is a cluster of blade computers that houses the majority of the software and computing power.

4.12.2 Thin Client Workstation Categories

a. There are three basic categories for the thin client workstations. The differences are the computer OS and the type hardware.

⁷⁸ DISA VTC STIG, Paragraph 6.3, Page 79.

b. Stateless Thin Client Workstation. These are thin client workstations, or terminals, that have no OS embedded on them. The limited software on them is firmware that is only sufficient enough to allow the terminal to connect across the network to the server. The OS and application software used by the client are run on the server. Only the keyboard, video monitor, and mouse updates are passed across the network between the client and server.

c. Embedded OS Thin Client Workstation. These are thin client terminals where the OS is embedded in the firmware. All application software and data reside on the server. As the OS is embedded in firmware, applying security patches is difficult as the terminal must be flashed with a new image. As the chipsets used in the firmware are OS specific, migrating or upgrading to a new OS is not possible without replacing the entire terminal.

d. Diskless Personal Computer (PC). These are regular desktop PCs that have had its internal hard drives removed. They are basically a stateless thin client on a different platform.

4.12.3 Thin Client Server Categories

a. The thin client back-end also has three basic categories, differing in the methodology they interact with the remote thin client terminals.

b. Terminal Services. Microsoft Windows Terminal Services is one of the more common methods, with other third party versions also available. All processing is done on the server, with only the user mouse and keyboard inputs and video screen updates being sent over the network.

c. Streaming OS and Applications. All of the processing is done on the terminal. When the terminal boots up, the server sends the OS to the terminal, and then each application as it's needed. In this setup, the terminals must be equipped with good processors and the network must be very robust.

d. Virtual Desktop. Everything is run on the server, which provides a virtual desktop to the remote terminal. Again, only user input and screen updates are passed over the network.

4.12.4 Thin Client Advantages

a. The decision to implement a thin client solution or not must be based on mission requirements and a thorough cost benefit analysis.⁷⁹ Thin client computing may offer substantial cost savings if properly designed and implemented. Typically, the initial capital

⁷⁹ Draft Memorandum, SAIS-AOI, Paragraph 6 plus Enclosures 1 & 2.

outlay for a thin client solution is much higher than for a standard computing solution due to the hardware, software, and licensing costs.

b. The reduction in Total Cost of Ownership (TCO) will occur over the life cycle of the system. Some of the factors that should be considered in determining the TCO are:

(1) Extended Hardware Life. The life of the thin client terminals is typically 4-5 years while a standard desktop computer or laptop is considered to be 3 years.

(2) Increased Mean Time Between Failures (MTBF). With fewer moving parts (such as no hard drives), the thin client terminals do not fail as often.

(3) Shorter Mean Time To Repair (MTTR). The thin client terminals can be replaced very quickly with no loss of data. The servers, which are typically redundant and/or backed--up regularly, can also be switched quickly, getting the user back into production in minimal time.

(4) Reduced Information Technology (IT) Staff. With longer MTBF, shorter MTTR, and centralized management and maintenance of the servers, fewer staff members are required to perform the maintenance.

(5) Reduced Non-Productive Time. The end users have more productive time available due to the longer MTBF and reduced MTTR.

(6) Reduction of Footprint. With some thin client solutions supporting Multi-Level Security (MLS) and Multi-Domain Security Solutions (MDSS), the need for multiple user terminals for different networks and classification levels is eliminated.

4.12.5 Thin Client Disadvantages

a. Network Connectivity. One important aspect of designing a thin client solution is the reliability, availability, and latency of the network connecting the thin clients to the servers. If the network fails, all users go down because they can no longer access the thin client server. In a standard computing environment, users still have access to the applications loaded on their particular machine that are not dependent on network connectivity when the network goes down. Thus, the total network dependence of the thin client solution is a real disadvantage if the local networks are not highly reliable.

b. Application Support. Another potential disadvantage is that some applications may not be designed to run well in a thin client environment. Computer-aided design (CAD) functions (used by a small number of SIPRNET users), as well as some legacy and highprocessing applications typically perform better on a traditional desktop computer. Careful planning and engineering are required to ensure the thin client solution meets the mission and user requirements before implementation.

c. Peripheral Devices. The use of peripheral devices at the user locations must be carefully considered in deciding to use a thin client solution. If peripherals such as a compact disk (CD) or digital video disk (DVD) drive are needed by a user, they must be provided as standalone units. Given the moratorium on universal serial bus (USB) storage devices in the Army, the use of local drives will not be possible without written exception to policy. Local printers attached to a terminal are also an issue. Thin client terminals are not equipped with serial or printer ports, so local printers need to be USB capable. The thin

client solution must account for this. Networked printers are the preferred solution in a thin client environment.

d. Data Leakage. Another important consideration in determining to use thin client is data leakage, especially in a classified environment. A thin client system typically provides a large data storage array that is partitioned into different network drives. All thin client users share the same physical drive. Without the appropriate network policies and procedures in place, data leakage may occur.

4.12.6 Thin Client System Requirements

a. Although a thin client solution can be ideal for use in a classified environment, several requirements must be met in the design and implementation of the system.

b. The SIPRNET connection for a thin client terminal, depending upon the type of access area it is located in (see <u>Paragraph 4.3</u>), may still require the use of PDS. The PDS shall be properly installed as outlined in this document.

c. The thin client terminals shall be diskless terminals that do not implement a full OS. $^{\rm 80}$

d. The thin client terminals shall support smart card readers, either integrated or USB connected, to enable login using the DOD Common Access Card (CAC).⁸¹

e. The thin client terminals shall support the Microsoft Windows Remote Desktop Protocol (RDP) as a minimum, for connection to the back-end servers.⁸²

4.13 Information Assurance (IA)

4.13.1 General

a. IA is the methods, procedures, and measures taken to protect the information stored, processed, accessed, or transmitted by ISs regardless of the classification of the information.

b. As addressed in this document, IA is specific to the construction, physical security, personnel activities, and processes related to the management and control of the SIPRNET infrastructure as discussed in this document. It is in no way implied that the criteria and recommended actions described in this document constitutes accreditation of or for the SIPRNET infrastructure. However, failure to follow these criteria and recommendations

⁸⁰ Draft Memorandum, SAIS-AOI, Enclosure 3, Paragraph 4.3.b.

⁸¹ Draft Memorandum, SAIS-AOI, Enclosure 3, Paragraph 4.3.c.

⁸² Draft Memorandum, SAIS-AOI, Enclosure 3, Paragraph 4.3.d.

will almost certainly result in non-accreditation as the criteria and recommendations are taken from the policies and regulations that must be followed to achieve accreditation.

The accreditation process is discussed further in Paragraph 5.2 of this document. c.

4.13.2 Information Security

a. All personnel involved in the generation, processing, transmission, or storage of the information are required to protect it commensurate with its classification level.⁸³ Classified information that is not under the direct personal control and observation of an authorized person must be appropriately guarded or stored in a locked security container or area appropriate for the classification of the material.⁸⁴

b. For classified information, all of the transmitted information must be encrypted using NSA Type 1 COMSEC devices,⁸⁵ be totally contained inside an open storage area approved at the Secret level, or be contained inside an approved PDS.

When installing a SIPRNET system, one aspect of information security that is often c. overlooked in the initial planning is the Information Assurance Vulnerability Management (IAVM) program. This is a proactive on-going program to ensure all ISs have all of the current required patches and updates to address vulnerabilities in its OSs, as well as to ensure other protective measures, such as host-based antivirus and firewalls, are current. This requires that qualified IT personnel be available and assigned to these duties. It is part of the O&M costs of a SIPRNET system.

d. The classified information generated, processed, transmitted, or stored in an IS is not always the only classified information that must be protected. At times, information about the IS itself may be classified, especially when the information is an aggregate of systems or a large amount of information even though the individual bits of information may be unclassified. Guidance in classifying data concerning the SIPRNET is given in DISA Circular 300-115-3.

4.13.3 Equipment Security

Equipment that directly stores classified information, such as computers, CDs, computer tapes, etc., is relatively easy to identify as having the capability of storing or retaining NSI. In the SIPRNET arena, such information is classified Secret. All equipment

 ⁸³ AR 380-5, Chapter 1, Paragraph 1-9, Page 3.
⁸⁴ AR 380-5, Chapter 7, Paragraph 7-4.a, Page 78.

⁸⁵ AR 25-2, Chapter 6 Paragraph 6-1.a, Page 52.

or media storing information must be clearly marked Secret.⁸⁶ In addition, they must be afforded the appropriate level of physical security during use and storage.

b. Other types of equipment that processes classified information, such as printers, photocopiers, and facsimile machines, have the capability to retain all or part of the classified information they processed. Any piece of equipment with this capability to retain the classified information must be afforded the same level of protection as the information itself, and again, it must be clearly marked as such. Many of these devices retain an image of the information only on certain parts of the equipment, such as the drums in a laser printer. While it is impractical to secure a large printer or other device that is not located in an open storage area, the information potentially stored on the equipment must still be protected. This may be accomplished by removing and properly storing only the parts of the equipment that could store classified information or by ensuring the potential image has been erased. The methods and procedures for doing this vary for each type and model of equipment. Actual procedures for securing these types of equipment must be coordinated with and approved by local IA personnel.

c. Access to the equipment and the information stored in the equipment must be controlled using layered security techniques to ensure only authorized personnel are granted access.⁸⁷ This must be done through a combination of physical and logical security measures. The measures taken to protect the classified information and equipment are part of the physical security aspect of the accreditation process.

5.0 SIPRNET CONNECTION PROCESS

5.1 DISN Connection Approval Process (CAP)

5.1.1 The DISN is the aggregate of the many global services provided by DISA. The DISN is comprised of the DRSN, DSN, DISN Leading Edge Services, DVS (which includes VTC capability), NIPRNET, Real Time Services (RTS) (which includes VoSIP), Cross Domain Solutions (CDS), and SIPRNET. The DISN CAP applies to a connection to any of these services. The overall flow of the DISN connection process is shown graphically in Attachment 6.⁸⁸

5.1.2 A new system or the expansion of an existing system, which requires a new connection to the SIPRNET WAN, or is of large enough scope to require re-accreditation,

⁸⁶ AR 380-5, Chapter 4.

⁸⁷ Access Control STIG, Paragraph 2.

⁸⁸ DISA Connection Process Guide, Figure 2, Page 3-2.

need to follow the CAP. An existing SIPRNET connection that is approaching the expiration date of its Authority To Connect (ATC) must also follow this DISN CAP, even in the absence of any type of changes to the system.⁸⁹ If the project is the expansion of an existing system using an existing connection and does not require re-accreditation, the CAP does not apply.

5.1.3 Supplemental information on the connection process for DVS and SIPRNET connections, along with points of contact at DISA, are given in Appendices E and I, respectively of the DISN Connection Process Guide. These appendices are reproduced in this document as <u>Attachment 7</u> (for the DVS CAP) and <u>Attachment 8</u> (for the SIPRNET CAP).

5.1.4 The DISN CAP specific to VoSIP, one of the RTSs provided by DISA, has not yet been incorporated into the overall DISN Connection Process Guide. As of the date of this document, the connection process guide for VoSIP remains a separate DISA document.

5.2 Accreditation and ATC

5.2.1 General

a. Accreditation is the official management decision by the DAA to allow an IS to operate. The DAA in so authorizing the system to operate accepts the risks inherent to the system and its attachment to the GIG. The DAA makes his decision based upon mission need and the recommendation from the Certification Authority (CA) as to whether the IS meets a prescribed set of security requirements. ⁹⁰ The accreditation goal for an IS is to achieve an Authority to Operate (ATO), which allows the system to operate. For some elements, such as with SIPRNET infrastructure, receiving proper accreditation is a precursor for receiving an ATC from DISA. This ATC is DISA's approval to connect your SIPRNET IS to the DISN SIPRNET WAN. Upon successful obtaining of at ATO and ATC, the SIPRNET IS can be connected and made fully operational to its users.

b. If the SIPRNET capability at a location is currently accredited, it must be reaccredited whenever it undergoes a major change. This could be as a result of a large expansion of the SIPRNET access service provided on an installation or a major change in the way that it is provided. Regardless of any changes, it must be re-accredited every three years.⁹¹

⁸⁹ DISA Connection Process Guide, Paragraph 3.2.1, Page 3-3.

⁹⁰ AR 25-2, Chapter 5, Paragraph 5-4.a, Page 49.

⁹¹ AR 25-2, Chapter 5, Paragraph 5-1.e, Page 48.

5.2.2 PDS Accreditation

a. The PDS installed as part of a SIPRNET access service is part of the overall SIPRNET IS. As such, it is part of the SIPRNET accreditation process. For accreditation purposes, the PDS must be approved.⁹²

b. Responsibilities concerning PDS will be shared between the responsible DAA and the Army CTTA, with the CTTA being a Technical Advisor to the DAA. Thus, the responsible DAA must approve a PDS, with recommendations from the Army CTTA, before a system can be accredited and placed into operation. The DAA has the authority to accept the risk of a PDS the Army CTTA finds to be non-compliant⁹³ based upon its threat versus cost analysis. The acceptance of a risk by the DAA must be done in writing, and is generally not recommended. In the interest of security, all non-compliant PDSs should be corrected as noted by the Army CTTA recommendations.

c. Prior to the implementation or modification of a PDS, during the planning stages, a technical review of the PDS must be requested from the Army CTTA. The request for a technical review of a PDS must be submitted by a Government official (not a contractor, although the contractor may be listed as a technical POC) via e-mail and must include all of the information required by NSTISSI 7003, Annex C.⁹⁴

d. Requests for approval of a PDS shall be forwarded to the DAA, and must include a copy of the technical review performed by the Army CTTA.⁹⁵ Note that the information required in the request is more than just the layout and construction of the PDS itself. The necessary information includes aspects of physical security and operational security procedures as well. The request to approve a PDS is classified at least at the Confidential level.⁹⁶

5.2.3 DOD Information Assurance Certification and Accreditation Process (DIACAP)

a. All ISs must be certified and accredited.⁹⁷ The process to certify and accredit an IS has been named DIACAP. The end result of the DIACAP is to obtain certification from the DAA the system is adequately secured and authorized to operate given the conditions and environment outlined in the DIACAP package.

⁹² AR 25-2, Chapter 6, Paragraph 6-2.b, Page 53.

⁹³ AR 380-27, Section 3, Paragraph 3-3.c.

⁹⁴ AR 380-27, Section 3, Paragraph 3-2.

⁹⁵ AR 380-27, Section 3, Paragraph 3-3.b.

⁹⁶ AR 25-2, Chapter 6, Paragraph 6-2.f, Page 53.

⁹⁷ DOD Instruction 8510.01

b. The DIACAP is a five-phase process that starts with the identification of the IS and its associated security requirements (IA controls), through Certification and Accreditation (C&A), and finally to sustainment and eventual system decommission. It may take months to go from initial system identification and description to achieving a system accreditation decision by the DAA. DIACAP is a detailed process that requires a team effort. For an Army installation, the NEC, as the system owner, is the organization responsible for obtaining and maintaining an accreditation that supports the installation campus area network (ICAN) and the ISs supported by the NEC that are included as part of the ICAN accreditation.⁹⁸

c. The accreditation approval discussed in previous paragraphs is part of the DIACAP.

d. The DIACAP results in a C&A package, which is ultimately submitted for approval to the Army CA. The Army CA, as appointed by the Army CIO/G6, is the Director, Cyber Security Division, CIO/G6 (recently changed from the Director, Office of Information Assurance and Compliance, NETCOM).⁹⁹ The Army CA is responsible for making recommendations to the DAA as to whether or not the IS should be accredited. The DAA then grants or denies the ATO based on those recommendations.

e. Once full accreditation has been achieved through the DIACAP, and the IS has been approved by the DISA CAO (the SIPRNET CAO, or SCAO for SIPRNET ISs), DISA will issue an ATC. Once the ATC has been granted, the system may be connected to the DISN SIPRNET WAN and is then fully functional and ready to provide service to the end users.

f. Additional details of the DIACAP are available in a paper written by Nova Datacom in 2009. That paper, with their permission, has been provided in this document as Attachment 9.

6.0 COST MODELING AND ESTIMATING FOR FINANCIAL PLANNING

6.1 General

6.1.1 After the initial design of a SIPRNET expansion project, the financial resources (i.e., the money) must be properly identified and obtained before the project can be implemented. The first step in this financial process is to estimate the cost of the project.

⁹⁸ AR 25-2, Paragraph 2-30.c.
⁹⁹ AR 25-2, Paragraph 3-3.n.
6.1.2 Cost estimation is an iterative process, in that it must be done several times as the design and financing of the project progresses. The initial cost estimate, based upon a very preliminary design, is by nature a gross estimation that is subject to change and revision. For the initial financial planning, a sample of a cost estimate developed using the gross cost estimation tool is provided in <u>Appendix I</u>. The tool provides a simplified means to obtain a mid-level cost estimate for a SIPRNET installation project using a PDS solution. It provides a starting point in the planning process. However, this tool should be used strictly for gross estimation purposes, such as determining an approximate cost for budgeting. The outcome should not be used to order materials or engineer the job. A site survey and engineering effort are required to refine the design and the cost estimate before procurement and implementation.

6.2 Cost Typing

6.2.1 General

a. All costs may be classified as either an expense or as an investment. Each is defined in subsequent paragraphs.

b. A system is comprised of a number of components that are part of, and function within, the context of a whole in order to satisfy a documented requirement. The system unit cost is the aggregate cost of all of the equipment and items acquired as the system.

c. The aggregate cost of a new end-item or system shall be used to determine whether it will be considered as an expense or an investment cost. If the costs are for the modification of hardware or software components of an existing system, only the additional procurement costs will be used in the determination whether the purchase is an expense or investment.¹⁰⁰

6.2.2 Expense

a. An expense is a cost that is incurred to operate and/or maintain the organization, such as equipment maintenance, personal services, supplies, and utilities. Expenses must be paid for using O&M, Army (OMA) funds.

b. Assemblies, spares, repair parts, and other items which have a system unit cost less than the currently approved threshold for expense/investment determination may be purchased as an expense.

¹⁰⁰ DFAS Manual 37-100-09, Appendix A, Para D.2.a and D.2.b.

c. Costs that are budgeted in O&M or military personnel appropriations are expenses.¹⁰¹

6.2.3 Investment

a. An investment is a cost that results in the acquisition or addition of end-items. These types of costs benefit future periods and generally are of a long-term nature, such as real or personal property. Investment costs must be paid for using Other Procurement, Army (OPA) funds.

b. All equipment items that have a system unit cost equal to or greater than the currently approved threshold for expense/investment determination must be purchased as an investment.

c. Costs that are budgeted in the Procurement, Research and Development, Test and Evaluation, or Military Construction appropriations are investments.¹⁰²

6.3 Funding Requirements and Limitations

6.3.1 General

a. The unit cost dollar threshold for expense and investment cost is \$250,000 for General Funds and \$100,000 for Army Working Capital Funds (AWCF). The threshold for accounting and capitalization is \$100,000 and is unchanged by the threshold for expense and investment costs.¹⁰³

b. The total system unit cost determines the type of funding that must be used. The validated requirement for the system may not be fragmented or acquired in a piecemeal fashion in order to circumvent the expense and investment criteria policy.¹⁰⁴

c. For SIPRNET installation or expansion type projects, the system unit cost includes the encryption devices, switches, PDS, cabling, and the equipment security housing. Whatever is required to satisfy the validated system requirement must be counted as part of the system unit cost.

d. O&M funds cannot be used to purchase any item, including replacement items, where the unit cost is more than \$250,000. If the total system unit cost exceeds \$250,000 then OPA funding must be used for procurement.¹⁰⁵

¹⁰¹ DFAS Manual 37-100-09, Appendix A, Para B.3.

¹⁰² DFAS Manual 37-100-09, Appendix A, Para B.3.

¹⁰³ DFAS Manual 37-100-09, Appendix A, Para 2.

¹⁰⁴ DFAS Manual 37-100-09, Appendix A, Para C.2.b.

6.3.2IT Procurement

a. When determining the total IT system cost, the labor cost to install the hardware and software must be included. 106

b. The cost for training and maintenance are normally separately funded using O&M funds, and must be if they are priced separately in a contract. If these costs are integral to the IT system contract cost and not broken out, they are then an integral part of the IT system cost and funded as part of the total system.¹⁰⁷

c. A LAN, CAN/MAN, or WAN are considered systems, so the total cost of all of the component parts must be used to determine the aggregate cost. Each level of network architecture (LAN, CAN, MAN, and WAN) is considered a separate system, so the costs for the procurement of each are separate¹⁰⁸.

d. Replacement of unusable components of a LAN system, such as substandard or non-functioning user drops, only the total cost of replacement is considered in determining the type of funds that may be used.¹⁰⁹ As long as the LAN system maintenance is below the threshold, O&M funds may be used.

e. Technology refreshment is the intentional incremental insertion of newer technology to improve reliability, improve maintainability, reduce cost, and/or add minor performance enhancements. The addition of such technology into end-items or systems as part of maintenance can be funded using O&M funds. However, technology refreshment that significantly changes the performance characteristics of the end-item or system is considered a modification and must be funded as an investment using OPA funds.¹¹⁰

f. Software licensing costs are considered part of the overall system cost for the initial purchase, and are thus, subject to the same funding constraints. Annual licensing costs thereafter are funded using O&M funds.¹¹¹

g. The funding source for a SIPRNET project may come from a variety of sources. The SIPRNET programs listed in this document (<u>Paragraph 4.1</u>) fund parts, or sometimes

¹⁰⁵ DFAS Manual 37-100-09, Appendix A, Para 1.d.

¹⁰⁶ DFAS Manual 37-100-09, Appendix A, Para D.1.c.

¹⁰⁷ DFAS Manual 37-100-09, Appendix A, Para D.1.d and D.1.e.

¹⁰⁸ DFAS Manual 37-100-09, Appendix A, Para D.3.c(3).

¹⁰⁹ DFAS Manual 37-100-09, Appendix A, Para D.2.b

¹¹⁰ DFAS Manual 37-100-09, Appendix A, Para C.3.d.

¹¹¹ DFAS Manual 37-100-09, Appendix A, Para D.3.c(2).

all, of a project. On some projects, portions may be funded by several different programs. Parts of a project that are not funded by a SIPRNET program must be funded by the organization that initiates the project. A generic breakdown showing which parts of a project are funded under the MCA program is shown in <u>Appendix K</u>.

APPENDIX A. FIGURES, DRAWINGS, AND DIAGRAMS

The figures, drawings, and diagrams follow.



Figure A-1. Example of WAN, MAN, CAN, and LAN



Figure A-2. SIPRNET High-Level Overview



Figure A-3. DISA-Managed SIPRNET Assets



Figure A-4. NEC-Managed SIPRNET Assets



Figure A-5. Tenant-Managed SIPRNET Assets

A-6



Figure A-6. SIPRNET Dial-Up Example





Figure A-7. PDS Physical Architecture Example



COMSEC COMSEC

Wireless Peer-to-Peer

Figure A-8. Wireless Architectures



Figure A-9. Secure-Only ISDN or IP VTC



Figure A-10. Multi-Domain ISDN or IP VTC

APPENDIX B. ENCRYPTION DEVICES

B.1 The choice of which encryption device to use in a particular project should be made based upon the capabilities of the device, the cost of the device, and the capability of local personnel to configure and manage the device. This appendix only provides information on the capabilities and availabilities of the devices.

B.2 Within the context of this document, the devices of interest are the INEs, the LEFs, and the keymat fill, or key loader, devices (part of the Key Management family). To aid in ordering COMSEC equipment from CSLA, Table B-1 provides National Stock Numbers (NSNs).

DEVICE	<u>NSN</u>		DEVICE	<u>NSN</u>		
Inline Network Encryptors (INEs)			Individual Mobile Encryptors & Wireless			
KG-175A	5810-01-527-9340	KC	DV-26 (card only)	5810-01-546-4543		
KG-175B	5810-01-527-9296	KC	OV-26 SOCOM Kit	5810-01-558-3251		
KG-175D	5810-01-547-4520	KC	OV-26 Office Kit	5810-01-558-5539		
KG-240	5810-01-529-4257	KC	OV-26 Tactical Kit	5810-01-558-5485		
KG-245	5810-01-533-4928	KC	OV-26 Executive Kit	5810-01-580-4740		
KG-245X	5810-01-568-9127	KC	OV-26 Adapter Upgrade	5810-01-76-8816		
K0-243A	3810-01-308-9127	Kit	t	3810-01-70-8810		
KG-250	5810-01-524-6615	KI	V-54 (with EM01)	5810-01-577-9979		
KG-255	5810-01-541-8542	KI	V-54 (with RM01)	5810-01-542-8334		
KIV-7MiP	NSN Pending	KI	V-11 (SecNet 11 Plus)	5810-01-538-3078		
Link Encryption Family (LEF)			Key Loading Devices			
KIV-7M	5810-01-530-2811	AN	N/CYZ-10 (DTD)	5810-01-393-1973		
KIV-7MiP	NSN Pending	AN	N/PYQ-10 (SKL) with	5910 01 517 2597		
KIV-19M	5810-01-548-8708	KC	DV-21	3010-01-317-3387		
KG-75A	5810-01-493-7871	AN	N/PYQ-10 (SKL) without	7010 01 517 2597		
KG-340	5810-01-582-8635	KC	DV-21	/010-01-31/-338/		

Table B-1. COMSEC Device NSNs

B.3 For each of the types of COMSEC devices (INE, LEF, and key loader), an evolution diagram is shown in Figure B-1.¹¹² The devices listed in the diagram in a green box are available and authorized for use. Devices listed in a yellow box are no longer available from the equipment manufacturer, but may still be available from CSLA, and may continue to be

¹¹² Army FY09 Crypto Modernization Program, Appendix D.

B-1

used. The CSLA ISSP website contains a list of recommended COMSEC devices based on the Crypto Modernization Program.

https://issp.army.mil/WebForms/Main.aspx (Requires AKO login to ISSP site.)



Figure B-1. Evolution of INEs

B.4 Availability and capability of various INEs are as shown in the above diagram and as described in the following paragraphs. Currently, all INEs used in Army networks must be compliant with HAIPE IS v3 or higher to be used.

a. KIV-11 (SecNet 11 Plus).

(1) The SecNet 11 Plus is an individual mobile encryptor that is designed to fit into a standard Personal Computer Memory Card International Association (PCMCIA) slot in a laptop or desktop computer for use as a secure wireless transmission link. It is manufactured by Harris RF Communications. The SecNet 11 Plus PCMCIA card is equipped with dual SMA connectors for the antennas.

(2) The SecNet 11 Plus implements a proprietary version of the 802.11b standard for Wireless communication links. As such, it is not interoperable with other wireless networking devices. Besides encrypting the classified data, the SecNet 11 Plus also encrypts the source and destination IP address information. With this unique feature, the use of WPA2 encryption is not required.

(3) The SecNet 11 Plus is not compliant with any version of the HAIPE IS due to its proprietary implementation of the 802.11b standard. It will not interoperate with any other wireless HAIPE device such as the SecNet 54 or the KOV-26 Talon.

(4) The link data rate of the SecNet 11 Plus match the standard 802.11b rates of 1 megabit per second (Mbps) to 11 Mbps. This is the transmission rate, which includes the entire user data packet plus overhead bits for IP and for wireless transmission. The actual user data rate will be substantially less.

(5) The SecNet 11 Plus protects the classified data from interception by encrypting it to NSA Type 1 standards. It may be used to protect classified information up to and including the Secret level. It is not authorized for use at the Top Secret level. The SecNet 11 Plus has a fill port on it for loading the keymat. It requires a special fill cable that is available from the manufacturer. The fill cable has a standard 5-pin connector at one end for interfacing with a standard key fill device.

(6) The SecNet 11 Plus is a CCI at all times. When it is unkeyed, it is unclassified as a Cryptographic Item (CI). Once keymat is loaded into it, the SecNet 11 Plus is classified to the level of the keymat. The hard drive of the classified computer used is classified, as it contains the classified information.

(7) A Wireless bridge desktop mounting case is available for the SecNet 11 Plus. When used in the wireless bridge mounting, the SecNet 11 Plus may be used as a wireless bridge between two classified wired networks when used in pairs. It may also be used as a WAP to allow multiple SecNet 11 Plus users to connect to a classified wired network via a wireless link.

b. KOV-26 Talon.

(1) The KOV-26 Talon is a modular individual mobile encryptor that is designed to fit into a standard PCMCIA slot in a laptop or desktop computer. It is manufactured by L-3 Communications. It consists of three basic parts: the Crypto Token, the Communications Adapter, and the Host Software. The crypto token is the KOV-26 card that plugs into the PCMCIA slot on a computer. The communications adapter is the dongle that plugs into the crypto token to provide the desired jack for compatibility with the chosen

SIPRNET Technical Implementation Criteria October 2010

transmission media. The host software is the software that must be run on the classified computer to enable it to work with the Talon.

(2) The KOV-26 has a standard USB interface that the communications adapter plugs into. Communication adapters are available for 10/100 Ethernet via a Registered Jack (RJ)-45, for IEEE 802.11b/g wireless links, a V.90 modem for dial-up applications, and an RS-232 serial adapter for interfacing to ISDN or other serial devices such as satellite communications terminals. Several kits are available for use with the KOV-26 to provide these capabilities. The office kit includes the KOV-26 and an Ethernet cable in a soft case. The tactical kit includes the KOV-26 and an Ethernet cable in a hard case. The Special Operations Command (SOCOM) kit includes the KOV-26, an Ethernet cable, and a fill cable in a hard case. The executive kit provides the KOV-26, a fill cable, and all four communications adapters in a hard case. An adapter upgrade kit is also available that provides the wireless, V.90 modem, and RS-232 serial adapters. Individual adapters are also available from the manufacturer.

(3) The actual data throughput of the KOV-26 Talon varies with the communications adapter used. Using the RS-232 adapter, the data throughput is up to 115.2 kilobits per second (Kbps). With the V.90 modem adapter, the data throughput is 56 Kbps. With the Ethernet or Wireless adapters, the data throughput is touted as 5 Mbps, although independent Government testing has only shown a rate of 2 Mbps.

(4) The KOV-26 protects the classified data from interception by encrypting it to NSA Type 1 standards. When the wireless adapter is used with the KOV-26, the wireless link must itself be encrypted using the WPA2 standard to protect the wireless link itself.¹¹³ A free software revision (Revision K) is available from the manufacturer to enable this capability. This revision must be implemented on all KOV-26 Talon cards, as well as the classified computers using the Talon software, both user and Site Security Officer (SSO), no later than 30 April 2011. This revision is available from the NSA SecurePhone website.

http://www.iad.gov/securephone (Requires CAC login to site.)

(5) The KOV-26 also has a fill port on it for loading the keymat. It requires a special fill cable that is available from the manufacturer. The fill cable has a standard 5-pin connector at one end for interfacing with a standard key fill device. The KOV-26 is rated for use with classified information up to and including the Top Secret level. It will store up to 384 PPKs and 8 Firefly keys.

¹¹³ DODI 8420.01, Enclosure 3 Paragraph 1.a.

(6) The KOV-26 is a CCI at all times, but is unclassified unless being used. When the KOV-26 has had classified keymat loaded into it, the KOV-26 is inserted into a PCMCIA slot, and a user has logged onto the card, then the KOV-26 is classified to the level of the keymat.¹¹⁴ The hard drive of the classified computer is classified, as it contains the classified information.

(7) The KOV-26, Release 1.1, is fully compliant with the HAIPE IS v1.3.5. Future free software upgrades from the manufacturer to HAIPE IS v3.1 are planned to be available around the end of 2011.

(8) The software used with the KOV-26 Talon has two versions, one for the user and one for the SSO. The user version is run on the user's computer to interface with the KOV-26. The SSO version is run on the SSO's computer only. The SSO has the ability to associate a KOV-26 with particular computers and users. Up to 15 user accounts may be programmed into one KOV-26, allowing it to be used by different users on different computers.

c. KIV-54 (SecNet 54).

(1) The KIV-54, also known as the SecNet 54, is a modular individual mobile encryptor. The KIV-54 is composed of the Cryptographic Module (CMOD), which encrypts/decrypts the information, and an external module which sends the encrypted information over the chosen transmission media. There are currently two types of external modules: the Ethernet Module (EMOD) and the Radio Module (RMOD). The KIV-54RM01 is the CMOD and the RMOD together, while the KIV-54EM01 is the CMOD and the EMOD together.

(2) The KIV-54 CMOD has dual inputs on the RED side, a standard RJ-45 port for copper, and Lucent Connectors (LCs) for multimode fiber optics. The RJ-45 copper port is 10/100 Mbps, the LC fiber port is 100 Mbps. The BLACK side of the CMOD interfaces directly to the external module for transmission of the BLACK signal. The overall size of the KIV-54 when the two modules are plugged together is 3.18 inches wide by 5.26 inches long by 1.13 inches thick. The CMOD is provided with an external power supply. It has dual power connectors so it can be used with redundant power supplies. It may also be powered through the RED-side RJ-45 jack using standard PoE technology. The KIV-54 uses 8 watts (W) of power maximum.

¹¹⁴ IDOC-016-06, Section 5 Paragraph 15.b

SIPRNET Technical Implementation Criteria October 2010

(3) The RMOD is provided with dual antennas that connect to it using standard Sub-Miniature version A (SMA) connectors. External antennas may be substituted if desired. The RMOD provides 802.11a/b/g wireless capability. With the provided antennas, the range of the wireless signal at full data rates is about 500 feet. At greater distances, up to 3,000 feet, slower data rates are achieved. The full speed data rate advertised is 54 Mbps. However, this is the transmitted data rate. The actual user data rate is much lower due to the encryption and packet overhead associated with wireless networking.

(4) Although the wireless side of the KIV-54RM01 is the encrypted (BLACK) side, the NSA Type 1 encryption only protects the classified information. It does not protect the wireless link itself. Therefore, the RMOD must always be operated using WPA2 encryption on the wireless link.¹¹⁵

d. KG-175 Classic and KG-175 E-100. Both of these devices are legacy devices that are still supportable by the manufacturer, General Dynamics C4 Systems. However, they are not upgradeable to HAIPE IS v3.x so they are not authorized for use. There is a trade-in program available whereby either of these legacy devices may be traded in for a newer KG-175D TACLANE Micro for a minimal cost (about \$7,000 as of the date of this document).

e. KG-175A GigE TACLANE.

(1) The KG-175A is the 1,000-Mbps Gigabit Ethernet device in the TACLANE family. It is HAIPE IS v1.3.5 compliant and has a software upgrade to HAIPE IS v3.1.2 available from the manufacturer.

(2) The KG-175A is a Gigabit Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber (LC). The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time.

(3) The GigE TACLANE will store 48 active PPKs plus 1 Firefly key. It may be used for classifications up to and including Top Secret.

(4) The GigE TACLANE is 1.73 inches high by 17.5 inches wide by 16.7 inches deep. It may be mounted in 1RU in a standard 19-inch rack/cabinet using the provided rack mount kit. It operates on 12 volts direct current (VDC) from an external power supply which draws 66 W of power. The power supply is auto-ranging, so it may be used with 120 volts alternating current (VAC) or 220 VAC. The power supply must be separately mounted in the rack/cabinet.

¹¹⁵ Memorandum, Asst Secretary of Defense, 2 June 2006, Attachment 1, Paragraph 1(1), Page 2.

f. KG-175B TACLANE Mini.

(1) Although the KG-175B is no longer produced by the manufacturer, General Dynamics C4 Systems, they are still providing support for this device. It may still be procured thru CSLA until stocks are exhausted. As such, it may still be used until further notice. There is a trade-in program available whereby a KG-175B may be traded in for a newer KG-175D for a minimal cost (about \$7,000 as of the date of this document).

(2) The KG-175B is HAIPE IS v1.3.5 compliant. A software upgrade to HAIPE IS v3.1.2 is available from the manufacturer.

(3) The KG-175B is a 100 Mbps Fast Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber (Mechanical Transfer Registered Jack [MTRJ]). The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time. The copper interfaces will operate at Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) while the fiber interfaces are Fast Ethernet only.

(4) The TACLANE Mini will store 48 chains (1 active plus 11 changeovers, for 1 year of operation) of PPK plus 1 Firefly key. It may be used for classifications up to and including Top Secret.

(5) The TACLANE Mini is 1.73 inches high by 8.25 inches wide by 17.25 inches deep, allowing one or two units to be rack-mounted in 1RU in a standard 19-inch rack/cabinet. It comes equipped with its own rack mount kit. It operates on 12 VDC from an external power supply which draws 75 W of power. The power supply is auto-ranging, so it may be used with 120 VAC or 220 VAC. The power supply must be separately mounted in the rack, although if only one KG-175B is mounted in a rack space, the power supply may be secured into the side of the rack mount kit.

g. KG-175D TACLANE Micro.

(1) The KG-175D is the latest version of the 100 Mbps Fast Ethernet TACLANE INE manufactured by General Dynamics C4 Systems. KG-175Ds are currently manufactured to HAIPE IS v3 compliance. Earlier manufactured units were HAIPE IS v1.3.5 compliant. A free software upgrade from the manufacturer is available for these units for HAIPE IS v3 compliance.

SIPRNET Technical Implementation Criteria October 2010

(2) As of 29 February 2009, all KG-175Ds are required to have been upgraded to manufacturers software Release 3.3v3 or later.¹¹⁶ Note that this software release is for the operating software embedded in the INE itself. The software upgrades for HAIPE compliance are separate upgrades.

(3) The KG-175D is a 100 Mbps Fast Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber (LC). The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time. The copper interfaces will operate at Ethernet (10 Mbps) or Fast Ethernet (100 Mbps), while the fiber interfaces are Fast Ethernet only.

(4) The TACLANE Micro will store 16 chains (1 active plus 11 changeovers, for 1 year of operation) of PPK plus 1 Firefly key. It may be used for classifications up to and including Top Secret.

(5) The TACLANE Micro is 1.61 inches high by 5.5 inches wide by 10.85 inches deep, allowing up to three units to be rack-mounted in 1RU in a standard 19-inch rack/cabinet. It requires the use of a rack mount kit which must be purchased separately. It operates on 12 VDC from an external power supply which draws less than 30W of power. The power supply is auto-ranging, so it may be used with 120 VAC or 220 VAC. If the rack mount kit is used to house three KG-175Ds, the external power supplies for all three must be separately mounted in the rack. For one or two KG-175Ds, the power supplies may be mounted in the rack mount kit along with the devices.

h. KG-235 Sectera. The manufacturer, General Dynamics C4 Systems, longer produces the KG-235 Sectera,. As of June 2009, it was no longer supportable.¹¹⁷ Thus, this INE is no longer authorized for use.

i. KG-240A RedEagle.

(1) The KG-240A is the latest version of the KG-240 100 Mbps Fast Ethernet INE manufactured by L-3 Communications, Communications Systems East. It is compliant with HAIPE IS v3.0.2. There is a no cost software upgrade from the manufacturer for HAIPE IS v3.1 compliance.

¹¹⁶ Memorandum, NSA, Subject: Notification of Mandatory Field Software Upgrade (FSU) to all TACLANE-Micro KG-175D In-Line Network Encryptors (INEs).

¹¹⁷ Army FY09 Crypto Modernization Program, Appendix D, Paragraph 8.b, Page 18.

(2) The KG-240A is a 10/100 Mbps Fast Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber (LC). The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time. The copper interfaces will operate at Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) while the fiber interfaces are Fast Ethernet only.

(3) The KG-240A will store 100 active PPKs plus 8 Firefly keys. It may be used for classifications up to and including Top Secret.

(4) The KG-240A is 1.61 inches high by 5.5 inches wide by 18.2 inches deep, allowing up to three units to be rack-mounted in 1RU in a standard 19-inch rack/cabinet. It requires the use of a rack mount kit which must be purchased separately. It operates on 12 VDC from an external power supply which draws 28W of power. The power supply is autoranging, so it may be used with 120 VAC or 220 VAC. If the rack mount kit is used to house three KG-240As, the external power supplies for all three must be separately mounted in the rack. For one or two KG-240As mounted in the dual rack mount kit, the rack mount kit is provided with power supplies integrated into it.

j. KG-245A RedEagle.

(1) The KG-245A is a Gigabit Ethernet encryption device in the RedEagle family manufactured by L-3 Communications, Communications Systems East. It is compliant with HAIPE IS v3.0.2. There is a no cost software upgrade from the manufacturer for HAIPE IS v3.1 compliance.

(2) The KG-245A is a 10/100/1,000 Mbps Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber (LC). The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time. The copper interfaces will operate at Ethernet (10 Mbps), Fast Ethernet (100 Mbps), or Gigabit Ethernet (1,000 Mbps) speeds while the fiber interfaces are Gigabit Ethernet only.

(3) The KG-245A will store 100 active PPKs plus 8 Firefly keys. It may be used for classifications up to and including Top Secret.

(4) The KG-245A is 1.61 inches high by 8.5 inches wide by 18.13 inches deep, allowing up to two units to be rack-mounted in 1RU in a standard 19-inch rack/cabinet. It requires the use of a rack mount kit which must be purchased separately. It operates on 12-36 VDC from an external power supply which draws 34 W of power. The power supply is auto-ranging, so it may be used with 120 VAC or 220 VAC. Two rack mount kits are available, one to mount two KG-245As with external power supplies, and one to mount a single KG-245A with integrated dual redundant power supplies.

k. KG-245X RedEagle.

(1) The KG-245X is a high-speed 10 gigabits per second (Gbps) Ethernet encryption device in the RedEagle family manufactured by L-3 Communications, Communications Systems East. It is HAIPE IS v1.3.5 compliant. There is a free software upgrade to HAIPE IS v3 available from the manufacturer. For units manufactured after March 2007, there is a free software upgrade to HAIPE IS v3.1.

SIPRNET Technical Implementation Criteria October 2010

(2) The KG-245X has a set of slots for small form factor pluggable (XFP) modules for the fiber optical interfaces on the RED and BLACK sides of the device. The type of fiber connectors depends upon the selection of the XFP fiber module used. The XFP fiber modules must be purchased separately.

(3) The KG-245X will store 100 active PPKs plus 5 Firefly keys. It may be used for classifications up to and including Top Secret.

(4) The KG-245X is 3.5 inches high by 17 inches wide by 17 inches deep. One unit may be rack-mounted in 2RUs in a standard 19-inch rack/cabinet using the provided rack mount kit. It operates on 120 VAC or 220/240 VAC automatically, and uses 250 W of power.

l. KG-250 AltaSec.

(1) The KG-250 is a 100 Mbps Fast Ethernet INE in the AltaSec family that is manufactured by ViaSat Inc. It is HAIPE IS v1.3.5 compliant. There is a free software upgrade from the manufacturer for HAIPE IS v3 compliance.

(2) The KG-250 has a set of copper RJ-45 interfaces that operate at either Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) speeds.

(3) The KG-250 uses 1 Firefly key. It may be used for classifications up to and including Top Secret.

(4) The KG-250 is 1.68 inches high by 7.5 inches wide by 11.9 inches deep, allowing up to two units to be rack-mounted in 1RU in a standard 19-inch rack/cabinet. It requires the use of a rack mount kit which must be purchased separately. It operates on 5 VDC provided by the rack mount kit. The rack mount kit contains an integrated power supply which draws 1A or less of current. The power supply is auto-ranging, so it may be used with 120 VAC or 220 VAC.

m. KG-255 AltaSec.

(1) The KG-255 is the Gigabit Ethernet device in the AltaSec family that is manufactured by ViaSat Inc. It is HAIPE IS v1.3.5 compliant and has a free software upgrade to HAIPE IS v3 available from the manufacturer.

(2) The KG-255 is a Gigabit Ethernet INE with dual interfaces. One set of interfaces is for copper cabling (RJ-45) and the other for fiber. The interface used, either fiber or copper, on each side of the device (RED and BLACK) is selectable, but only one interface on each side may be used at a time. The RJ-45 copper interface operates at Fast Ethernet (100 Mbps) or Gigabit Ethernet (1,000 Mbps) speeds. The fiber interfaces are slots for small form factor pluggable (SFP) modules, which must be purchased separately. The type of fiber optic connector used is dependent upon the SFP module used.

(3) The KG-255 can be used with either PPK or Firefly keymat. It may be used for classifications up to and including Top Secret.

(4) The KG-255 is 1.72 inches high by 17 inches wide by 19.8 inches deep, allowing it to be rack-mounted in 1RU in a standard 19-inch rack/cabinet using the rack mount kit provided. It operates on 120 VAC or 220/240 VAC using an integrated power supply. The power supply draws a maximum of 89 W of power.

B.5 Availability and capability of COMSEC devices in the LEF are as shown in Figure B-2 and as described in the following paragraphs. Previous members of the LEF, such as the KG-81, KG-94, KG-194, and KG-95, are obsolete and are no longer authorized for use.¹¹⁸

a. KIV-7M.

(1) The KIV-7M is link encryption device manufactured by SafeNet Inc. It is a direct replacement for previous models of the KIV-7 (KIV-7HS, KIV-7HSA, and KIV-7HSB). The previous models are no longer manufactured, but are still supportable by the manufacturer. They should not be used in new circuits or installations.



¹¹⁸ Army FY09 Crypto Modernization Program, Appendix D, Paragraph 8.a, Page 16. B-11

Figure B-2. Evolution of LEF

(2) The KIV-7M is a multi-purpose programmable dual-channel link encryption device. Each of the two channels is independently programmable, giving it the same capacity as two of the link encryption devices that it replaces.

(3) Each channel of the KIV-7M will operate at a different, or the same, security classification using different keymat for each channel, up to and including Top Secret. The KIV-7M will store up to 10 active PPKs.

(4) The KIV-7M channels operate at speeds up to 50 Mbps for synchronous data. They can be programmed to one of three different electrical interface standards: EIA-530 (RS-449), RS-232, and EIA-644 (LVDS). With the optional DS3 module, it will interface with industry standard DS3 trunk circuits. The DS3 module is directly interoperable with the KIV-19M link encryption device.

(5) The KIV-7M is 1.71 inches high, 5.88 inches wide, and 11.01 inches deep, using up only half of a 1RU rack space. A separately purchased rack mount kit allows up to two KIV-7Ms to be mounted in 1.83 inches (slightly more than 1RU) in a standard 19-inch rack or cabinet. The KIV-M consumes a maximum of 11 W of power and operates from 5 VDC provided by the power supply integrated into the rack mount kit. The rack mount power supply operates from 120 VAC or 220/240 VAC automatically, and consumes a maximum of 200 W of power when operated with two devices in it.

(6) The DS3 module is the same size as the KIV-7M and can be mounted in the same rack mount kit.

b. KIV-7MiP.

(1) The KIV-7MiP is the newest in the KIV-7 series manufactured by SafeNet Inc. It is basically a KIV-7M with RJ-45 network ports added to provide an IP capability. It is the first COMSEC device capable of operating simultaneously as a link encryptor and an INE.

(2) All three channels (two links, one network) are independently programmable and capable of operating at different or identical security classifications with separate keymats. The network channel is HAIPE IS v1.3.5 compliant, upgradeable to v3.1. It will operate at Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) speeds.

(3) The KIV-7MiP can be operated using PPK or Firefly keymat up to and including Top Secret.

(4) The form factor is the same as the KIV-7M, enabling it to use the same rack mounting kits.

(5) As of the date of this document, the KIV-7MiP has not been authorized for Army use. It is currently undergoing testing by the Communications-Electronics Research Development and Engineering Center (CERDEC). Pending completion of testing and approval for Army use, it has not been assigned a NSN and is not available for purchase from CSLA.

c. KIV-19M.

(1) The KIV-19M is a ruggedized, programmable, dual-channel link encryption device manufactured by Sypris Electronics. It is a direct replacement for previous models of

the KIV-19 (KIV-19 and KIV-19A). The previous models are no longer manufactured and are not supportable. They are no longer authorized for use.

(2) The KIV-19M channels operate at speeds from 9.6 Kbps to 50 Mbps. They can be programmed to one of three different electrical interface standards; MIL-STD-188-114A (Type 2 Balanced), RS-422, or EIA-644A (LVDS). Each of the two channels in the KIV-19M can be independently programmed. The KIV-19M is directly interoperable with the KIV-7M/MiP.

(3) Each channel of the KIV-19M will operate at a different, or the same, security classification using different keymat for each channel, up to and including Top Secret. The KIV-19M can use PPK or Firefly keymat.

(4) The KIV-19M is 1.7 inches high, 5.9 inches wide, and 10.8 inches deep, using less than half of a 1RU rack space. Separately purchased rack mount kits allow either two or three KIV-19Ms to be mounted in 1RU in a standard 19-inch rack or cabinet. The dual rack mount kit contains an integrated power supply. The triple rack mount kit uses and external power supply that must be separately rack-mounted. The KIV-19M consumes a maximum of 50 W of power in the rack mount kit. The power supplies for the rack mount kits operate from 120 VAC or 220/240 VAC automatically. A desktop mounting kit with integrated power supply is also available.

d. KG-75A FASTLANE.

(1) The KG-75A FASTLANE is the updated version of the KG-75 manufactured by General Dynamics C4 Systems. It provides link encryption for Asynchronous Transfer Mode (ATM) and SONET links. The KG-75 base model is no longer authorized for use.

(2) The KG-75A operates as an ATM/SONET device at data rates of Optical Carrier (OC)-3 (155.52 Mbps), OC-12 (622.08 Mbps), or OC-48 (2.488 Gbps), or as an ATM-only device at the OC-192 (10 Gbps) speed.

(3) The KG-75A will store up to 64 chains (1 active plus 11 changeovers) of PPK and 22 Firefly keys at a time. It can be used for encrypting data up to and including the Top Secret level. To provide a measure of operational security, the KG-75A "stuffs" ATM cells into the data stream to maintain a constant transmission rate when the actual data to be transmitted drops to low levels.

(4) The KG-75A is 7.25 inches high by 17.50 inches wide by 21.50 inches deep and can be mounted in 4RUs in a standard 19-inch rack/cabinet using the mounting kit provided. It will operate from 120 VAC or 220 VAC automatically, and consumes 150-240 W of power depending on the data transmission interfaces used.

(5) The KG-75A may be remotely managed by the General Dynamics family of remote management software also used with the KG-175 TACLANE family of INEs.

e. KG-189.

(1) The KG-189 is an ATM/SONET encryption device that was originally manufactured by Motorola and later by General Dynamics. While it is no longer manufactured, it is still supportable, so it may remain in use until further notice.

(2) The KG-189 operates at data rates of OC-3, OC-12, or OC-48, and may be used to encrypt classified data up to and including Top Secret.

(3) The KG-189 is 21.3 inches wide by 27 inches high by 23 inches deep and weighs approximately 70 lbs. It may be directly mounted in a standard 23-inch rack/cabinet, the size typically found in large telecommunications facilities. As it was designed for use in a large telecommunications facility like a Dial Central Office, it operates from 48 VDC and uses 265 W of power.

f. KG-340.

(1) The KG-340 is a high-speed link encryption device manufactured by SafeNet, Inc. It is designed for use in SONET networks at speeds from OC-3 (155.52 Mbps) up to OC-192 (10 Gbps). The KG-340 has SFP slots for the interfaces, so the fiber optic connectors used are dependent upon the SFP module used. The modules are purchased separately.

(2) The KG-340 uses the Firefly keymat and may have up to 192 separate security associations, one for each STS-1 channel in an OC-192 trunk.

(3) The KG-340 is 3.5 inches high by 19 inches wide by 23 inches deep, allowing it to be mounted in 2RUs in a standard 19-inch rack/cabinet using the integrated rack mount kit. Designed for use in a large telecommunications facility, it operates from 48 VDC power. It has dual power inputs for redundancy.

B.6 Availability and capability of key loader devices are as shown in <u>Figure B-3</u> and as described in the following paragraphs.

a. CYZ-10 DTD.

(1) The CYZ-10, often called the "Crazy 10," was manufactured by Sypris Electronics, LLC. It is no longer in production, but remains a valid key loading device that is still authorized for use. It is a portable, hand-held fill device for securely receiving, storing, and transferring data between compatible cryptographic and communications equipment.

(2) The CYZ-10 is 3.5 inches wide by 6 inches deep by 1.7 inches thick when opened for operation. It weighs about 4 lbs. The user interface is a 35-button keypad below the liquid crystal display (LCD) window, which only displays 2 lines of 24 characters each. The interface to the COMSEC device is the standard military 6-pin circular connector.

b. PYQ-10 SKL.

(1) The PYQ-10 SKL is the newest key loading device in the Army inventory and is the replacement for the older CYZ-10. It is manufactured by Sierra Nevada Corporation.

(2) The PYQ-10 is basically a ruggedized special purpose handheld computer. It operates using the Windows Embedded Compact (CE) OS. The user interface is the navigation buttons below the 3.5 inch LCD or a stylus. The PYQ-10 is 4.25 inches wide by 7.45 inches deep by 2.25 inches thick. It is operated by power from a replaceable battery and is provided with a battery charger that operates from 120 VAC or 220 VAC automatically. The interface to the COMSEC device is the standard military 6-pin circular connector.



Figure B-3. Evolution of Key Management

This page intentionally left blank.

APPENDIX C. PDS INSPECTION CHECKLIST

INSTRUCTIONS				
Install Team Check or "X" each item in the "Install Check" column to indicate you have checke and it meets the criteria. Enter "N/A" for items that do not apply to the site installation.				
QA Team	Check or "X" a "Go" or "No Go" next to each item. All "No Go" marks should be described on the TAR deficiencies sheet. Put "N/A" in the "Go" column for items that do not apply to the site installation. A mark in the "QA Fix" column next to a "No Go" means that the "No Go" was fixed during the QA inspection and is now a "Go".			

PDS INSPECTON CHECKLIST							
Project:							
Location:							
Inspector Name: Date:							
ITEM		ITEM DESCRIPTION / CRITERIA		QA	QA Inspection		
#				GO	NO GO	QA FIX	
1	General Layout						
А	The SIPR document	NET room layout is as defined in the final planning					
В	All last mi and appro installation	nute changes from the designed layout coordinated with ved by the Project Manager or Project Engineer prior to the n.					
С	The UDBs per user.	s are spaced to allow a minimum of 3 ft of working space					
D	The work picked up	site was left in a clean condition (all dust, dirt, and debris), as good as if not better than when the installation began.					
2	PDS Carri	er & UDBs	•				
А	All carrier	is installed level/vertical.					
В	The carrie attachmen	r is held away from the wall using at least 1/2" at every t point.					
С	The hardw installed a	vare used to attach the carrier to the wall is properly nd tightened.					
D	All UDBs (Assuming	All UDBs are installed the same height above the floor $\pm 1/4$ " (Assuming floor is level. If not, use $\pm 1/4$ " of true level line.)					
Е	All carrier dents.	All carrier and UDBs are free from visible nicks, scratches, and dents.					
F	The door on each UDB closes without binding.						
G	One S&G changed fi	lock is secured on each UDB with the combination rom the manufacturer standard (25).					
Н	UDBs hav pulled at l	e enough cable slack inside to allow the faceplates to be east 6" away from the UDB.					
Ι	Cables ins at least 1" connector.	ide the UDBs are individually labeled (Drop1, Drop2, etc.) from the connector but no more than 4" from the					
J	The cables cable shea	s are properly terminated in the connectors, crimped on the th, with no wires visible out the back of the connector.					
K	Each netw combined over the so easily rem	ork connection is individually labeled on the faceplate (no labels such as "Drop 3/4") and the labels are not adhered crews used to secure the faceplate, leaving the faceplate ovable.					

PDS INSPECTON CHECKLIST						
Project:						
Location:						
Inspector Name:			Date:			
ITEM			T (H	QA	Inspec	tion
#		ITEM DESCRIPTION / CRITERIA	Check	GO	NO GO	QA FIX
L	All of the same way					
М	The door cable entry the wall.	on the PDS box on the back of the IPS that covers the Red ance opens and closes without binding and does not scrape				
Ν	If Holocor locking ki	m duct is used, the pull release cable for the first Holocom t is accessible inside the PDS box on the rear of the IPS.				
3	IPS Conta	iner				
Α	IPS is free	e of major scratches, scrapes, and marring.				
В	IPS comb (50-25-50	ination has been changed from the manufacturer standard				
С	One S&G the IPS with standard (lock is secured on top of the PDS box door on the back of ith the combination changed from the manufacturer 25), with the dial facing up for easy viewing.				
D	The PDS towards th between the PDS box	box over the Red cable entrance is turned so that it opens he room, not the side wall, unless there is enough space he IPS and the side wall to stand in the space to open the without having to lean over the IPS.				
Е	The "Loc	ked/Open" magnetic plaque is on the front of the IPS door.				
F	The rack I All bolts a plate.	ocking plate is installed to secure the rack inside the IPS. and washers are present and used to secure the locking				
G	The rack rails are present and stored next to the IPS					
Н	The air fil using the 2 IPS, the "6 the IPS.	ter is secured over the air intake vent on the hinge side 2 supplied clips. If using the older, longer, version of the ear muffs" are installed over the air vents on both sides of				
I	There is a other obst using the each side be, and the	t least 2 1/2" of space between the air vents and the wall or ruction next to the IPS, to allow for adequate air flow. If older, longer, version of the IPS, there is sufficient space on of the IPS to allow the "ear muffs" to be removed if need e door on the PDS box can be fully opened.				
J	Excess A power out box, not o	C power cable between the back of the IPS and the wall let is neatly coiled and secured. It is run under the PDS ver it, if the AC outlet is to the hinge-side of the IPS.				
К	Inside the both the b secured.	rear of the IPS, the interior security combs and covers for lack and red cable entrance boxes are properly installed and				
4	AC Power	r Cabling Inside IPS Container				
А	The AC p the rear of does not c	ower cable for the UPS is plugged into the power strip in the IPS and is fastened to the rack at the top corner. It ross the red user drop cable bundle.				
В	When the mechanism loosen it of	rack is slid all of the way to the end of the track m, there is not sufficient pull on the AC power cable to or to pull on the power strip in the rear of the IPS.				

PDS INSPECTON CHECKLIST						
Project:						
Location:						
Inspector Name:			Date:			
ITEM		ITEM DESCRIPTION / CRITERIA		QA	Inspec	ction
#				GO	NO GO	QA FIX
С	When the does not f rack base	rack is slid fully back into the IP, the UPS power cable all in such a way as to be pinched between the rack and the in the rear of the IPS.				
D	The AC p the rear st	ower cable for the UPS is neatly routed and secured down rike-side vertical rack rail.				
Е	In the rear from the e secured to	of the rack, the remaining equipment AC power cables, equipment to the back of the UPS, are neatly routed and the rack.				
5	Red User	Drop Cabling Inside The IPS				
А	The red us where the the moval	ser drop cables are neatly secured together in a bundle from y enter the IPS to the rack. It is secured to the top corner of ble rack and does not cross the AC power cable.				
В	With the r bundle ha extended,	ack fully extended on the track mechanism, the cable s only a slight sag in it. If the rack cannot be fully this item is a "no go."				
С	When the does not f rack base	rack is slid fully back into the IPS, the red cable bundle all in such a way as to be pinched between the rack and the in the rear of the IPS.				
D	Any excess cable in the red user drop cables is neatly coiled inside the PDS box on the back of the IPS not inside the IPS					
Е	The red cable bundle is routed and securely fastened inside the rack from the top corner at the back of the rack to the connections on the equipment/patch panel.					
F	Each red the equipt sheath, wi	user drop cable is properly terminated in the connector at nent/patch panel. The connector is crimped on the cable ith no wires visible out the back of the connector.				
G	Each red of from the c	cable is individually labeled (Drop1, Drop2, etc.) at least 1" connector but no more than 2" from the connector.				
6	Red Signa	Il Cabling Inside The IPS				
А	All other of ends at lea connector	cables, such as patch cords, are individually labeled at both ast 1" from the connector but no more than 2" from the .				
В	For all cal on a connector maintenar	bles inside the IPS, there is no undue stress or pull placed ector due to the way it is routed and secured. Each cable may be easily unplugged from the equipment for nce and testing purposes.				
С	No cables an empty	are routed across the face of another piece of equipment or rack space.				
D	If cable tie cable tie a protruding	es are used, all of the tails sticking out of the head of the are cut flush with the head so there are no short/sharp ends g.				

This page intentionally left blank.

APPENDIX D. SAMPLE SIPRNET SITE SURVEY CONSIDERATIONS

A sample SIPRNET site survey considerations follows.

SIPRNET SITE SURVEY CHECKLIST

			Date:	
Complete all	parts of the survey checklist b	below. Use additional	sheets and attachments as requi	red.
Facility Nam	ne			
Facility Loca	ntion (include both mailing	& physical if differer	nt):	
Mailing:	Street:			
	City:	State:	Zip:	
Physical: Stre	eet1:			
	Street2:			
	City:	State:	Zip:	
If more than	l building in the facility, wha	t is the building numbe	er/designation?	
SITE SURV	EY PERSONNEL			
Gov	vernment:			
Cor	ntractor:			
SIPRNET R	oom #:			
Is the designation	ted SIPR room currently rate	d for Secret level open	storage? (Y/	N)
Communicat	tions Room servicing the SI	PR room:		
Commercial	Telephone Demarc Room f	or Building:		
		D-2		
	FOR OFF	ICIAL USE	ONLY	
POINTS OF CONTACT

List as many POCs as are, or will be, involved in this project. The Primary and Alternate POCs should be personnel in the building to receive SIPRNET service. Also list the installation/facility communications personnel. To show which POCs were actually part of the site survey, indicate next to their e-mail whether they were present or not.

Primary POC	Name:	
At SS:	E-mail:	
	Phone: Office:	Cell:
Alternate POC Name:		
At SS:	E-mail:	
	Phone: Office:	Cell:
NEC/G6 POC Name:		
At SS:	E-mail:	
	Phone: Office:	Cell:
NEC/G6 POC Name:		
At SS:	E-mail:	
	Phone: Office:	Cell:
Fac Engr POC Name:		
At SS:	E-mail:	
	Phone: Office:	Cell:
Other POC	Name:	
At SS:	E-mail:	
	Phone: Office:	Cell:

D-3 FOR OFFICIAL USE ONLY

EXISTING SIPRNET

Is th	ere an existing SIPRNET connection?		(Y/N) (If no, skip this section)
Тур	e of connection (dialup, T1, 256K, etc.):		
For	other than dialup, what is the CCSD?		
Whe	ere is the existing SIPRNET located in the f	acility?	
List	the make & model of all equipment used:		
Nun	ber of user devices (PCs, laptops, printers,	etc.)?	

If the plan is to have two or more separate groups of users in the facility, describe how they will all be linked together to the building SIPRNET point of presence.

Military Installation NEC/G6/Base Comm Information:

Note the location of the post demarc, both building number and physical street address / location:

If other than the standard clear (pale yellow upon drying) epoxy color is required, note that fact. For Holocom duct, note if epoxy will be required or not, or if a waiver applies.

If any specific equipment is required for connection to the local CAN, such as modems or media converters, note the make and model with any special additions or modules.

Discuss all of the responsibilities involved with the local installation communications POC and note any changes or additions. Continue on the back as needed.

Provide all Red IP addresses needed.
Provide Black IP addresses needed.
Configure/baseline laptops/computers.
Provide IAVA & AV monitoring & updates.
Provide & load FireFly key into INE.
Configure INE and switch after installation.
Establish connectivity between INEs.
Update accreditation if required.

Building Floor Plan

Obtain a copy of the facility floor plan. If a drawing is not available, a fire escape plan will suffice. The floor plan must show the SIPRNET room, the commercial telephone demarc room, and the route between them.

Floor Plans Obtained?	Yes	No		(check one)
IPS Delivery	Is a loadi	ng dock av	ailable (Y/N	IJ?
Are there any barriers pro	otecting the	entrance (Y	//N)?	
Is the exterior door on th	e ground flo	or (Y/N)?		
If not, how many steps u the Cyber Café room?	p to the entra	ance most a	accessible to)
Note the construction of	the steps (ma	aterial).		
How wide are the stairs?		_		
For higher floors, is there	e an elevator	(Y/N)?		
If so, is it large enough &	k strong enou	ugh for the	IPS (Y/N)?	
If not, note the following	g for the stair	s from the	ground floo	r.
Number of flights of stai	rs			
Number of stairs in each	flight _			_
Construction of the steps	3			
Width of stairs				
		D-6		

SIPRNET Technical Implementation Criteria October 2010

N	umber of landings in each stairwell
S	hape & size of each landing
 N	fote the floor covering inside the SIPRNET room
1	
N Cy	tote the floor covering along each part of the route from the entrance door used for the IPS ber Café
C	heck the doorways along the route. Are any doors under
3	2" of clearance between the jambs? If so, note them on
tł	the facility floor plan, with the clearance dimension. (Y/N)
С	heck the hallways along the route. Are any hallways less
tł	an 60" measured between the baseboards? If so, note them
0	n the facility floor plan with the clearance dimension. (Y/N)
If	the café is not on the ground floor, what is
tł	he maximum static floor loading, in lbs/sq ft?
If	the café is not on the ground floor, has the DPW or
E	ngineer POC provided written or e-mail assurance
tł	hat the floor will support the IPS? (Y/N)
	Attach the document to these site survey notes.)

t (size, material, spacing, orientation, etc.)

PDS Carrier Note the type of PDS carrier to be used.

Note the height of the ceilings in all hallways.

Note the heights of the ceiling in all rooms with PDS.

Note the type construction and thickness of the walls where PDS will be installed.

On a floor plan, for each room that will receive a UDB, where in the room the UDB will be placed. Next to it, note the height above finished floor (AFF) that the UDB will be installed at.

Also on the floor plan, draw the route that the PDS will follow. Note any obstructions to be avoided. Note where the PDS must make a change in elevation around obstacles on the walls.

TEMPEST Note the location, make, and model of all fixed transmitters and antennas located in the facility or within 30 feet of the facility (in all 3 dimensions).



SIPRNET Room Floor Plan

Draw a detailed, dimensioned, floor plan of the room to be used to house the IPS container. This is the beginning of the PDS.

Draw in all columns, windows, and doors.

Clearly mark on it where the IPS container will be located, and its orientation (show door swing). Ensure sufficient wall clearance is available around the IPS for ventilation.

Mark the location of all electrical outlets.

Note the location of all non-classified network drops.

Note the wall construction to determine the type of anchor needed.

Note any wall obstructions along the PDS carrier route that are more than 1/2" out from the wall.

Note any furniture or equipment that will need to be moved (by facility personnel) prior to the arrival of the IPS.

Ensure the ceiling height is noted on the drawing, as is the ceiling type (drywall, concrete, drop). If a drop ceiling, note the space between the drop and true ceiling.

Site Preparation: Check each that apply (ref AR 380-5). Add notes on back as appropriate.

- Entrance door(s) are not solid core or metal clad (need to be replaced).
- Entrance door(s) open outward (hinges need pinned/brazed).
- _____ Door lock(s) should be replaced with high security lock(s).
- _____ Window in door(s) (needs covered with bars/grating & obscured).
- _____ Vent in door(s) (needs covered with bars/grating & soundproofing).
- Exterior window(s) in room (need covered with bars/grating).
- Exterior window(s) in room (need obscured paint/curtain/blinds).
- _____ Not enough AC outlets for IPS & users (need AC added to room).
- Café has door into an adjacent room (check is door to adjacent room or doors/windows in adjacent room need to be secured).

The café room has air conditioning to keep the room at or below 85F.

T1 Circuit Info:

If an existing SIPRNET capability is to be used, skip this section. Complete this section only if a new SIPRNET circuit from DISA is required. The following information will be needed by the DISA Circuit Implementation team after they have engineered the circuit. Once they have designed the circuit, sending them this information will help to speed their planning and installation process.

In the SIPRNET room, is there an existing cable entrance through the walls, possibly above the drop ceiling, that could be used to run the T1 circuit in? If so, note its location, size, and percent fill with other cables on the floor plan drawing.

Follow the cable path from the building demarc room to the SIPRNET room and draw it on a copy of the facility floor plan. Note the type of ceiling and wall construction along the pathway, as well as the approximate cable distance. Note the ceiling heights along the entire route. For areas with drop ceilings, also note the distance from the drop ceiling to the true ceiling above it.

If there are any intermediate walls along the pathway that need to be penetrated, note their construction and thickness. If there are existing wall penetrations, note their location, type (conduit, hole, etc.), size, and percent fill.

Make a floor plan of the building demarc room. Note where the demarc connector blocks are located. Note the commercial cable identification (if known) and the number of pairs. Note the type of lightning protection blocks used as well as the type of distribution connection blocks they feed into. Write down the make and model number of the lightning protection block used, the size (50 pair, 100 pair, etc.), and the type of cross-connect blocks that it feeds into (R66, 110, wire wrap, etc.).

This page intentionally left blank.

APPENDIX E. SIPRNET USER AND ALLOCATION TABLES

Office	Title	Drops	Connections
Command, Brigade	Commander	1	2
Command, Brigade	XO	1	1
Command, Brigade	CSM	1	1
		3	4
S-1	Brigade S-1	1	3
		1	3
S-2	Brigade S-2	1	4
		1	4
S-3, Ofc of Chief	Brigade S-3	1	2
S-3, Training	Brigade S-3 Training	1	1
S-3, Opns Div	Brigade S-3 Ops	1	2
S-3, Ops, MOB Br	Brigade S-3 MOB	1	2
		4	7
S-4	Brigade S-4	1	3
		1	3
S-6, Ofc of Chief	Brigade Signal Officer	1	1
S-6 Info Svc Div (ISD)	Brigade S-6 ISD		1
S-6, Plans & Ops Div	Brigade S-6 Plans & Ops		1
		1	3
Conference Room	Conference Room	1	2
		1	2
HHD	Commander	1	2
		1	2
	TOTAL	13	28

 Table E-1. User Allocation and Distribution at Brigade HQ BCT

Office	Title	Drops	Connections
Command, Battalion	Commander	1	2
Command, Battalion	ХО	1	1
Command, Battalion	SGM	1	1
		3	4
S-1	Battalion S-1	1	1
		1	1
S-2	Battalion S-2	1	2
		1	2
S-3	Battalion S-3	1	2
		1	2
S-4	Battalion S-4	1	1
		1	1
S-6	Battalion S-6	1	1
		1	1
Conference Room	Conference Room	1	2
		1	2
	TOTAL	9	13

Table E-2. User Allocation and Distribution at Battalion BCT

Office	Title	Drops	Connections
Office of CG	Commander	1	2
Office of CG	Deputy Commander	1	2
Office of CG	Deputy Commander	1	2
Office of CG	Aide-de-Camp		
Chief of Staff	Chief of Staff	1	1
SGS	Secy General Staff	1	1
CSM	Div CSM	1	1
		7	9
G-1	DCS, G1	1	3
		1	3
G-2	DCS, G2	1	2
	Plans	1	2
	Future Ops		1
	Recon & Surveillance	1	1
		3	6
G-3, Office of Chief	DCS, G3	1	2
G-3, Plans	Deputy G3 Plans	1	2
G-3, Operations Div	Deputy G3 Ops	1	2
G-3, Training	Deputy G3 Tng	1	1
G-3, Ops, MOB Br	Ch, MOB Br	1	1
		5	8
G-4, Office of Chief	DCS, G4	1	1
	G4 Ammo	1	1
	G4 MOB		1
		2	3
G-6, Office of Chief	DCS, G6	1	2
G-6, Info Svc Div (ISD)	Supv Info Tech	1	1
G-6, Plans & Ops Div	Commo Off	1	2
		3	5
G-8	G8 Comptroller	1	2
Command Surgeon	Surgeon	1	1
PAO	PAO	1	1
Command Chaplain	Command Chaplain	1	1
SJA	SJA	1	1
IG	IG	1	1
Conference Room	Conference Room	1	2
HHD	Cmd	1	1
		8	10
	TOTAL	29	44

Table E-3. User Allocation and Distribution at Division HQ

Office	Title	Drops	Connections
Office of CG	Commander	1	2
Office of CG	Deputy Commander	1	2
Office of CG	Deputy Commander	1	2
Office of CG	Aide-de-Camp	-	_
Chief of Staff	Chief of Staff	1	1
SGS	Secy General Staff	1	1
CSM	Corps CSM	1	1
	Colps Colm	7	9
G-1	DCS G1	1	3
0-1	DC5, 01	1	3
6.2	DCS G2	1	2
0-2	DCS, 02	1	2
	Fialls	1	2
	Puture Ops	1	1
	Recon & Survemance	1	1 C
	DOI 01	3	0
G-3	DCS, G3	1	2
	Deputy G3 Plans	1	2
	Deputy G3 Operations	1	2
	Deputy G3 Training	1	1
	Ch, MOB Br	1	1
		5	8
G-4	DCS, G4	1	1
	G4 Ammo	1	1
	G4 MOB		1
		2	3
G-6	DCS, G6	1	2
	Information Services Div	1	1
	Plans & Ops Div	1	2
		3	5
G-8	G8 Comptroller	1	2
Command Surgeon	Surgeon	1	1
Public Affairs Office	Public Affairs Officer	1	1
Cmd Chaplain	Command Chaplain	1	1
SJA	SJA	1	1
IG	IG	1	1
Conference Room	Conference Room	1	2
HHD	CMD	1	1
Corps MI		1	1
Corps MP		1	1
Corps ADA		1	1
Corps Avn		1	1
Corps Engr		1	1
Corps Arty		1	1
		14	16
	ΤΟΤΔΙ	35	50
	IUIAL	35	50

Table E-4. User Allocation and Distribution at Corps HQ

Office	Drops	Connections
School Commandant	1	1
Assistant Commandant	1	1
Deputy Assistant Commandant	1	3
Deputy Assistant Commandant Army Reserve		
Deputy Assistant Commandant National Guard		
Chief of Staff	1	3
Aide de Camp		
CSM		
U.S. Army Engineer School		
Training Brigade	1	2
Directorate of Training Development	1	1
Department of Development Support	1	2
Directorate of Combat Developments	1	2
TRADOC System Manager		
TRADOC Program Integration Office		
Directorate of Training		
Total Army School System Division		
Doctrine Development Division		
Department of Instruction		
Branch Personnel Proponency Office		
Directorate of Plans and Operations	1	1
Personnel Proponency		
Test and Evaluation Office		
TOTAL	9	16

Table E-5. User Allocation and Distribution at School Commandant and U.S. ArmyEngineer School

Table E-6.	User Allocation and Distribution at Depot Commander and Production
	Operations

Office	Drops	Connections
Depot Commander		
Deputy to the Commander	1	1
Chief of Staff	1	2
Depot Sergeant Major		
Production Operations		
Director of Production		
Director of Mission Plans and Operations	1	1
Director of Production Engineering		
Director of Risk Management	1	1
Director of Law Enforcement and Security	1	2
Director of Quality Improvement		
Depot Operations Office	1	1
Director Systems Integration and Support		
TOTAL	6	8

Table E-7. User Allocation and Distribution at Garrison Commander and Garrison Directorates

Office	Drops	Connections
Office of the Garrison Commander		
Garrison Commander	1	1
Deputy to the Commander	1	2
CSM		
Garrison Directorates		
Plans, Analysis and Integration Office (PAIO)	1	1
Resource Management Office (RMO)	1	1
HHC/HHD, U.S. Army Garrison		
Directorate of Human Resources (DHR)		
Directorate of Morale, Welfare and Recreation		
(DMWR)		
Directorate of Plans, Training, Mobilization and	3	6
Security (DPTMS)	-	-
Directorate of Emergency Services (DES)	1	1
Directorate of Logistics (DOL)	1	1
Directorate of Public Works (DPW)		
Directorate of Information Management (DOIM)	3	6
Installation Legal Office (ILO)	1	1
Public Affairs Office (PAO)		
Religious Support Office (RSO)		
Installation Safety Office (ISO)	1	1
Equal Opportunity Office (EOO)		
Internal Review Office (IRACO)	1	1
Installation Contracting Office (ICO)	1	1
TOTAL	16	23

APPENDIX F. SIPRNET ALLOCATIONS FOR NEW MILITARY CONSTRUCTION

	<u> </u>	SIPRNET FOR NEW 1	MILITARY (UCTION	
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	COMMENTS
CODE	SUB	DESCRIPTION	NUMI	KEQ D	(IME or INE)	COMMENTS
111		Airfield Runways	N			
112		Airfield Taxiways	N			
113		Airfield Aprons	N			
116		Other Airfield Pavements	Ν			
121		Aircraft Fuel Dispensing Facilities	Ν			
122		Marine Fuel Dispensing Facilities	N			
123		Land Vehicle Fuel Dispensing Facilities	N			
124		Operating Fuel Storage Facilities	N			
125		Petroleum, Oil, and Lubricant Pipeline	Ν			
126		Other Liquid Fuel and Dispensing Facilities	Ν			
131		Communications (Information Systems) Buildings	Y	Y	INE	
132		Communications Facilities Other Than Buildings	Ν			
133		Aviation Navigation and Traffic Aids Bldgs	Y	Y	INE	
134		Aviation Navigation and Traffic Aids Facilities Other Than Buildings	N			
135		Communications Lines	N			
136		Airfield (Heliport) Pavement Lighting	Ν			
137		Ship Navigation and Traffic Aids Buildings	Y	Y	INE	
138		Ship Navigation and Traffic Aids Other Than Buildings	Ν			
141		Operational Buildings	Y	Y	INE	
142		Helium Plants and Storage	Y	Y	INE	
143		Ship Operational Buildings	Y	Y	INE	
149		Operational Support Facilities Other Than Buildings	Ν			
151	1	Piers and Wharfs	Ν			
154		Sea Walls, Bulkheads, and Quay Walls	Ν			
155		Small Craft Berthing	N			

Table F-1. SIPRNET for New Military Construction

SIPRNET FOR NEW MILITARY CONSTRUCTION						
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS
156		Cargo Handling Facilities and/or Buildings	Y	Y	INE	
159		Other Waterfront Operational Facilities	N			
163		Moorings	Ν			
164		Marine Improvements	Ν			
171		Training Buildings	Y	Y	INE	
172		Simulation Facilities	Y	Y	INE	
177		Impact, Maneuver, and Training Areas	N			
178		Training Ranges	Y	Y	INE	Drill down to only digital range facilities
179		Training Facilities Other Than Buildings	Y	Y	INE	Drill down to only digital range facilities
211		Aircraft Maintenance Facilities	Y	Y	INE	
212		Guided Missile Maintenance Facilities	Y	Y	INE	
213		Ships and Spares Maintenance Facilities	Y	Y	INE	
214		Tank and Automotive Maintenance Facilities	Y	Y	INE	
215		Weapons and Spares Maintenance Facilities	Y	Y	INE	
216		Ammunition, Explosives, and Toxics Maintenance Facilities	Y	Y	INE	
217		Electronics and Communications Equipment Maintenance Facilities	Y	Y	INE	
218		Miscellaneous Items and Equipment Maintenance Facilities	Y	Y	INE	
219		Installation, Repair, and Operations Maintenance Facilities	Y	Y	INE	
221		Aircraft Production Facilities	Y	Y	INE	
222		Guided Missiles Production Facilities	Y	Y	INE	
224		Tank and Automotive Production Facilities	Y	Y	INE	
225		Weapons and Spares Production Facilities	Y	Y	INE	

SIPRNET FOR NEW MILITARY CONSTRUCTION						
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS
226		Ammunition, Explosives, and Toxics Production Facilities	Y	Y	INE	
228		Miscellaneous Items and Equipment Production Facilities	Y	Y	INE	
229		Installation Maintenance and Repair Production Facilities	Y	Y	INE	
310		Research, Development, Test, and Evaluation (RDT&E) Science Laboratories	Y	Y	INE	
311		Aircraft RDT&E Buildings	Y	Y	INE	
312		Missile and Space RDT&E Buildings	Y	Y	INE	
314		Tank and Automotive RDT&E Buildings	Y	Y	INE	
315		Weapons and Weapons Systems RDT&E Buildings	Y	Y	INE	
316		Ammunition, Explosives, and Toxics RDT&E Buildings	Y	Y	INE	
317		Electronic and Communications Equipment RDT&E Buildings	Y	Y	INE	
318		Propulsion RDT&E Buildings	Y	Y	INE	
319		Miscellaneous Items and Equipment RDT&E Buildings	Y	Y	INE	
321		Technical Services RDT&E Buildings	Y	Y	INE	
371		RDT&E Range Facilities	Y	Y	INE	
390		RDT&E Facilities Other Than Buildings	N			
411		Bulk Liquid Fuel Storage	N			
412		Liquid Storage Other Than Water, Fuel, and Propellants	N			
421		Depot and Arsenal Ammunition Storage	N			
422		Installation and Ready- Issue Ammunition Storage	N			
423		Liquid Propellant Ammunition Storage	Ν			

SIPRNET FOR NEW MILITARY CONSTRUCTION						
-	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS
424		Weapon-Related Battery Storage	N			
425		Open Ammunition Storage pad	N			
431		Depot and In-Transit Cold Storage	Ν			
432		Installation and Ready Issue Cold Storage	Ν			
441		Depot and Arsenal Covered Storage	Ν			
442		Installation and Organizational Covered Storage	N			
451		Depot Open Storage	N			
452		Installation and Organizational Open Storage	Ν			
510		Medical Centers and Hospitals	Y	Ν	IME	1 Drop
530		Medical and Medical Support Facilities (Laboratories)	N			
540		Dental Clinics	Ν			
550		Dispensaries and Clinics	Y	N	IME	1 Drop (If no hospital (under Cat 510))
610		Administrative Buildings	Y	Y	INE	
	61001	Military Entrance Processing Station (MEPS)	Y	Y	INE	
	61002	Recruiting Station: Storefront	Y	N	IME	
	61050	Administrative Building, General Purpose	Y	Y	INE	
	61055	Waiting Area/In-Out Processing	N			
	61065	Technical Library	N			
	61070	Red Cross Building	Ν			
	61075	Courtroom	Ν			
620		Underground Administrative Structures	Y	Y	INE	
690		Administrative Structures Other Than Buildings	N			
711		Family Housing: Dwellings	N			
	71111	Family Housing: General Officer	Y	Ν	IME	
	71112	Family Housing, Colonel	Ν			

SIPRNET FOR NEW MILITARY CONSTRUCTION							
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION		
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS	
	71113	Family Housing, LT Colonel and Major	N				
	71114	Family Housing, Company Grade and Warrant Officer	N				
	71115	Family Housing, Senior NCO	Ν				
	71116	Family Housing, Junior NCO/Enlisted	Ν				
	71117	Family Housing, Other Than Military	Ν				
712		Family Housing: Trailers	Ν				
713		Family Housing: Trailer Sites	Ν				
714		Family Housing Support Facilities	Ν				
720		Transient Housing	N			Possible	
721		Enlisted Personnel Unaccompanied Personnel Housing	N				
722		Unaccompanied Personnel Housing Mess Facilities	Ν				
723		Detached Unaccompanied Personnel Housing Facilities	N				
724		Officers Unaccompanied Personnel Housing	Ν				
725		Emergency Unaccompanied Personnel Housing	Ν				
730		Personnel Support and Service Facilities	Ν				
	73015	Confinement Facility	Y	Y	INE	Warden	
	73016	Police/MP Station	Y	Y	INE	MP	
	73017	Chapel	Y	Ν	IME	Chaplain	
740		Indoor Morale, Welfare, and Recreation Facilities	Ν				
	74010	Auditorium, General Purpose	Y	N	IME	Deployment Purposes (IME or Roll- about)	
	74028	Physical Fitness Center	Y	N	IME	Deployment Purposes (IME or Roll- about)	
	74034	Community Activities Center	Y	N	IME	Deployment Purposes (IME or Roll- about)	

SIPRNET FOR NEW MILITARY CONSTRUCTION						
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS
750		Outdoor Morale, Welfare, and Recreation Facilities	N			
760		Museums and Memorials	Ν			
811		Electrical Power Source	Ν			
812		Electrical Power Transmission and Distribution Lines	N			
813		Electrical Power Substations and Switching Stations	N			
821		Heat Source	N			
822		Heat Transmission and Distribution Lines	N			
823		Heating Gas Source	N			
824		Heating Gas Transmission	N			
826		Refrigeration (Air- Conditioning) Source	N			
827		Chilled Water (Air- Conditioning) Transmission and Distribution Lines	Ν			
831		Sewage and Industrial Waste Treatment and Disposal	Ν			
832		Sewage and Industrial Waste Collection Lines	N			
833		Refuse and Garbage Facilities	N			
834		Landfills	N			
841		Potable Water Supply, Treatment, and Storage	Ν			
842		Potable Water Distribution System	Ν			
843		Fire Protection Water Facilities	Ν			
844		Nonpotable Water Supply and Storage	Ν			
845		Nonpotable Water Distribution System	Ν			
846		Water Storage: Potable	N			
847		Water Storage: Non- potable	Ν			
851		Roads	N			
852		Sidewalks and Other Pavements	Ν			
857		Training Area Roads	N			
860		Railroad Tracks	N			
861		Railroad Facilities Other Than Track	Ν			

SIPRNET FOR NEW MILITARY CONSTRUCTION						
	CA	TEGORY	SIPRNET	PDS	ENCRYPTION	
CODE	SUB	DESCRIPTION	RQMT	REQ'D	(IME or INE)	COMMENTS
871		Grounds Drainage	N			
872		Grounds Fencing, Gates, and Guard Towers	N			
880		Fire and Other Alarm Systems	Ν			
881		Fire Extinguishing Systems	Ν			
891		Miscellaneous Utilities Measured in SF	Ν			
892		Miscellaneous Utilities Measured in Each	Ν			
893		Miscellaneous Utilities Measured in Linear Feet	Ν			
894		Miscellaneous Utilities Measured in Cubic Feet Per Minute	N			
895		Miscellaneous Utilities Measured in Gallons	Ν			
911		Land Purchase, Condemnation, Donation, or Transfer	N			
912		Public Domain Withdrawal	Ν			
913		License or Permit	Ν			
914		Public Land of Territories and Possessions	Ν			
915		Land Purchase, Donation, or Transfer to State (National Guard Use Only)	Ν			
921		Easements	N			
922		In Lease	N			
923		Foreign Rights	N			
932		Clearing, Grading, and Landscaping	Ν			
933		Demolition of Facilities	Ν			
934		Cut and Fill	Ν			
940		Contaminated Facility or Area	N			
IME = Indiv	vidual Mo	bile Encryption Device				
IMEs are pr	oposed fo	or buildings with 10 or less				
users.						

This page intentionally left blank.

APPENDIX G. SAMPLE SOP FOR SIPRNET CONNECTIONS

A Sample SOP for SIPRNET Connections follows.

FORT COVERT

STANDING OPERATING PROCEDURE

FOR

SIPRNET CONNECTIONS

Effective 19 December 2005

TABLE OF CONTENTS

1. PURPOSE	3
2. REFERENCES	3
3. EXPLANATION OF TERMS	3
4. APPLICABILITY	3
5. RESPONSIBILITIES AND PROCEDURES	3
APPENDIX A. TABLE OF DISTRIBUTION AND ALLOWANCES ACCOUNT ORDER CCI EQUIPMENT	6
APPENDIX B. COMSEC CHECKLIST	7
APPENDIX C. SIPRNET CHECKLIST	11
APPENDIX D. INFORMATION ASSURANCE MGR (IAM) DRAFT CERTIFICATION MEMORANDUM	13
APPENDIX E. IATO AND DITSCAP	14
APPENDIX F. FORT COVERT ACCEPTABLE USE POLICY	15
APPENDIX G. DIAL-UP ACCOUNT	19

Fort Covert SOP No: ####

- 1. PURPOSE: Procedures to establish SIPRNET connection at Fort Covert
- 2. **REFERENCES**:

a. BBP 03-EC-0-0001: Acquiring Secret Internet Protocol Router Network (SIPRNET) Connectivity: Version 1.0

- b. AR 25-2, Information Assurance
- c. AR380-5, Information Security Program

d. AR380-40, Policy for Safeguarding and Controlling Communications Security – (COMSEC) Material

- e. Army Regulation 381-14; Military Intelligence, Technical Counterintelligence, (C)
- 3. EXPLANATION OF TERMS:

CCI: Controlled Cryptographic Item COMSEC: Communications Security CRM: Customer Relationship Manager DIACAP: DOD Information Assurance Certification and Accreditation Program DOIM: Director of Information Management IA: Information Assurance IAM: Information Assurance Manager IASO: Information Assurance Security Officer IATO: Interim Authority to Operate IMO: Information Management Officer ISSP: Information Systems Security Program SIPRNET: Secret Internet Protocol Router Network TCC: Telecommunications Center TDA: Table of Distribution and Allowances

- 4. APPLICABILITY: To establish SIPRNET connection.
- 5. **RESPONSIBILITIES and PROCEDURES:**

a. Organization Point of Contact (POC) will contact the DOIM CRM for that organization requesting a SIPRNET connection.

b. CRM will assist the requesting Organization POC with initiating the requirements gathering to prepare a project proposal and notify the DOIM SIPRNET manager of a request for SIPRNET connectivity.

c. The CRM will set up a meeting between the Organization POC, the Organization Security Officer, CRM, a representative from the Installation Security Office or IA representative, and a representative from the Secure Network Group to gather requirements and set up a meeting for a site inspection. IA Representative will inspect the proposed location to determine if it meets the requirements for classified processing (in accordance with AR380-5). If not approved, the Installation Security Office or an IA representative will provide the Organization POC a written list

of deficiencies and carbon copy (cc) the CRM. The Secure Network Group Representative will discuss the different CCI equipment available and will work with the Organization POC to determine how the CCI equipment will be procured through the organization's ISSP (must have an approved TDA account if CCI equipment is a TDA item). (See Appendix A) The organization makes a decision on what approved CCI equipment they plan to procure and notify the Secure Network Group. An equipment list of required parts for crypto ancillaries, cabling, fiber modems, and router information including costs will be provided to the CRM from the Secure Network Group for the installation. The CRM in turn notifies the Organization POC.

d. If Open Storage is a requirement the Organization Appointed Security POC will need to be contacted.

e. Upon decision as to the type of equipment to be used and type of connection, the Secure Network Group will notify the COMSEC Custodian of the new keying requirement. COMSEC Custodian will do a site survey with the Organization POC.

f. The COMSEC Custodian will contact the Organization POC to set up the requirement for a hand receipt (Appendix B – COMSEC Custodian).

g. The IA Representative will request from the Organization POC the name of the IASO for the SIPRNET node. The process will not continue until this information has been established and provided to the IA Representative.

h. The IA Representative will contact the IASO and provide the IASO website address for IASO training certification before the system can be activated. At this time the IA Representative will notify the IASO of the DIACAP requirements and provide a go-by.

i. The CCI Equipment Hand Receipt Holder will notify the CRM and the IA Representative when the required CCI equipment has been received. The IA Representative will contact the IASO to determine the status of the DIACAP. If an IATO is required, the IASO, through the IMO, will request one.

j. The IA Representative will re-inspect the location to ensure the configuration meets the physical and security requirements per regulation. The IA Representative will provide the following to the DOIM SIPRNET PM:

SIPRNET Checklist (See Appendix C)

Information Assurance Manager (IAM) Certification Memo verifying that all requirements have been met (See Appendix D)

IATO or DIACAP (See Appendix E)

k. Upon approval of either the IATO or the DIACAP, the IA Representative will notify the CRM and Secure Network Group that the system can be connected. At this time, the Secure Network Group will connect the organization, transfer the equipment to the appropriate organization hand receipt holder, and do a one-on-one briefing on the crypto equipment.

1. The Organization POC will submit DD Form 2875 (original with signatures) to the IA Section for all individuals requesting access to SIPRNET. Upon verification, the IA personnel will give the DD Form 2875 to the TCC where the individual accounts will be created in accordance with Garrison Policy SOP 1-1. The TCC will notify the individual when the account is ready for pickup.

SIPRNET Technical Implementation Criteria October 2010

At the time of pickup and prior to an individual signing for a login and password, the individual will be required to acknowledge understanding the SIPRNET Acceptable Use Policy (SAUP) (See Appendix F) by reading and signing the SAUP. The individual will then be permitted to sign for the login and password.

m. Once the Organizational user receives a login, the user will be responsible to submit to the Help Desk to have the SIPRNET system (i.e. desktop, laptop) setup and configured.

n. If an organization requires a dial-up SIPRNET account, the user will need to register through the user's IASO who will sign off on their security measures and validate the requirement. (See Appendix G)

APPENDIX A. Table of Distribution and Allowances Account

1. To acquire an approval for a Table of Distribution and Allowances (TDA) account, follow AR 71-32 Appendix E-3 and E-4.

· Fort Covert POC; John Smith @ ext. xxxx

Order CCI Equipment

2. To order CCI equipment:

a. Your IAM, IAPM, IASO (or other personnel who encompasses any position types that do not fall into one of the types listed and generates requirements) needs to input your ISSP requirement into the Information System Security Program (ISSP) Database. The ISSP POCs at CSLA are Ms. Charity Torrez, (520) 538-8381, DSN: 879-8381, Josh Crider, -1829, and TJ Lindroos, -8460, e-mail cslaissp@csla.army.mil

NOTE: TO RECEIVE COMSEC EQUIPMENT AS AN ARMY ORGANIZATION, THE REQUIREMENT MUST BE ENTERED IN THE ISSP. EQUIPMENT REQUIREMENTS THAT WILL BE UNIT-FUNDED OR DA-FUNDED MUST ALL BE ENTERED INTO THE ISSP.

b. If the unit will be utilizing an INE and has received approval, the MIPR should to be addressed through CSLA to NSA and include the ISSP requirement ID number which will validate your ISSP Requirement. Once the MIPR is received, it is processed and forwarded to NSA who puts the purchase on contract. Currently, normal delivery of the INE is 4-5 months (after the purchase is put on contract). Please put your ISSP requirement ID number in the body of the MIPR. Ensure that the Property Book Officer (PBO) processes the MIPR with a Document Number.

APPENDIX B. COMSEC

Fort Covert DOIM 19 December 2005

STANDING OPERATING PROCEDURE OBTAINING COMSEC KEYING MATERIAL

PURPOSE: This DOIM Garrison Army Standing Operating Procedure (SOP) outlines procedures for obtaining COMSEC keying material from the DOIM Garrison and the guidelines and responsibilities for COMSEC hand receipt holders.

REFERENCES:

1. AR 380-40 (Policy for Safeguarding and Controlling Communication Security (COMSEC) Material

2. TB 380-41 (Technical Bulletin)

3. AR 380-5.

4. AR 71-9.

5. AR 381-14 (C)

1. GENERAL INFORMATION.

- APPROVED SECURITY CONTAINER
- USE OF COVER SHEETS
- VERIFY CLEARANCE AND NEED TO KNOW
- PRACTICE GOOD SECURITY!
- USE SF 701 (ACTIVITY SECURITY CHKLIST)
- USE SF 702 (SCTY CONTAINER CHKLIST)

1.1. Media. The protection of classified information, whether printed material,

computer hard drives, or COMSEC keying material, is the responsibility of each individual who has knowledge or possession of that information, regardless of how that knowledge was obtained.

a. Whenever classified information is not under the personal control or observation of an authorized person, it will be secured in an approved security container, vault, or area approved for classified open storage.

b. Material removed from storage will be covered with a classified document cover sheet (SF 703, 704 or 705) when not in secure storage, especially when carried between offices, placed in internal distribution centers, or placed in in/out boxes, etc.

c. The material will be destroyed in accordance with the procedures established for classified material of when no longer needed.

d. Personnel must always ensure proper security clearance and need to know prior to providing classified defense information to any individual.

1.2. COMSEC Material. COMSEC material must be stored in an approved container when not under the personal control or observation of an authorized person (the COMSEC Hand Receipt holder or alternate as designated by forms attached to this SOP, submitted to and approved by the DOIM COMSEC Custodian). Only these personnel can possess COMSEC material or have access to the storage container which stores COMSEC material. Do not share access to this container with non-authorized personnel.

2. RESPONSIBILITIES:

2.1. All personnel must ensure compliance with this instruction for handling and controlling COMSEC materials. The primary DOIM COMSEC Custodian will ensure all COMSEC Hand Receipt Holders are trained and briefed annually, as a minimum. All personnel who have COMSEC material on hand receipt must be relieved from accountability through the DOIM COMSEC account 30 days prior to their departure.

3. PROCEDURES:

3.1. Request for new service. All new service requests should come from or be directed by the Organization's CRM. The Garrison DOIM COMSEC custodian should be brought in as early as possible on the requirements analysis and solution design process for all new service requests -- preferably on the initial CRM/Customer meeting. After SIPRNET solution design has been decided by DOIM Network Services Team, and concurrently while customer is awaiting equipment delivery, IAM approval of the customer's physical security site, and sign-off granting an authority to connect, the following COMSEC requirements must be met:

a. Organization's User representative must request site to be approved as a COMSEC storage facility. The "COMSEC Facility Approval" form is attachment _____.

b. If Site does not have a COMSEC hand receipt holder, the customer must ensure one is properly appointed, trained, and briefed. Request package is enclosed as attachments_____, ____, and ____.

c. If contractor personnel are assigned as the COMSEC hand receipt holder or alternate, a copy of the contract's DD254 (which documents that user has valid requirement) and a "Visit Request" must be provided to the Garrison DOIM COMSEC custodian.

d. DOIM COMSEC Custodian will advise customer/CRM concerning requirement for ancillary equipment needs to ensure devices can be successfully keyed.

e. Customer will submit a properly completed "Request for Keying Material" form to the Garrison DOIM COMSEC custodian. Customer will be advised on expected lead times for acquiring requested key material.

f. Before customer's encryption devices will be activated, the COMSEC custodian must:

1) Receive from the customer a completed "Hand Receipt Holder Checklist" (see attachment ____)

2) Grant COMSEC storage site approval for the customer's site, and

3) Receive written authorization from the DOIM IAM granting approval for site connection to the SIPRNET.

Upon arrival of customer's COMSEC keying material, customer will be notified to arrange pickup. When circuit connectivity is completed, DOIM WAN Team will coordinate going "hot" with customer and DOIM COMSEC custodian.

3.2. COMSEC Facility Approval Request. If the COMSEC keying material is to be stored in the area where the encryption devices are located, Organization must submit a facility request and be granted approval by the DOIM COMSEC custodian. Your request can be faxed or hand-carried to the DOIM COMSEC custodian. COMSEC material must be stored in a GSA-approved safe.

G-9

3.3. Hand Receipt Holder (HRH) Procedures. Requesting Organization should choose a primary and at least one alternate person to be COMSEC hand receipt holders. Once package is approved, HRH or alternate is authorized to sign for COMSEC material. These personnel should be involved in the day-to-day operation of the circuit so that the DOIM COMSEC custodian, IAM, or WAN Team can easily contact them for status, troubleshooting, or to communicate pertinent information. Once HRH request package is approved, the DOIM COMSEC custodian will arrange a time and place to conduct initial brief as to their duties in handling COMSEC material.

3.4. COMSEC Material Request. After receiving facility and HRH approval, COMSEC keying material for customer's encryption devices can be ordered. Organization must submit a "COMSEC Material Request" to the DOIM COMSEC custodian. COMSEC custodian will then order the necessary keying material from CLSA using the justification provided by the user on his request. Strength of justification can considerably influence the length of time it takes for key material to arrive.

3.5. Rekeying and Support. All cryptographic equipment must be electronically rekeyed annually at a minimum; some devices requiring monthly keying. Additionally, all devices can potentially lose their key at any time due to lightning, power failure, etc. All devices terminating with the DOIM are monitored daily; however, if your device does fail, contact the TCC to request assistance. The DOIM COMSEC Custodian or alternate will contact you and provide verbal instructions on rekeying your devicef situation cannot be resolved over the phone, they or a member of the WAN Team will visit your site to diagnose the problem.

COMSEC Checklist

STEP	ACTION	DATE Submitted or Received	Customer Initials	DATE Submitted or Received	DOIM COMSEC Custodian Initials
1	COMSEC Facility Approval Request				
	SUBMITTED to DOIM COMSEC				
	Custodian?				
2	COMSEC Facility Approval Request				
	APPROVED by DOIM COMSEC				
	Custodian?				
3	DD254 and Visit Letter received for				
	Contractors (if applicable)				
4	Hand Receipt Holder Guide				
	SUBMITTED to DOIM COMSEC				
	Custodian?				
5	Copy of signed HRH Guide approved				
	and given to HRH				
6	IATO or DIACAP and Physical				
	Security approved by DOIM IAM				
	(Written proof required)				
7	HRH and Alternate Briefed as to their				
	duties and responsibilities by DOIM				
	COMSEC Custodian?				
8	Ancillary Equipment information				
	provided (if applicable)				
9	COMSEC Material Request				
	SUBMITTED to the DOIM				
	COMSEC custodian.				
10	COMSEC Material Request				
	APPROVED by the DOIM COMSEC				
	custodian.				

Organization:

SITE Location:

User Representative:

Phone #:

COMSEC Custodian validates SITE Ready to go HOT?

SIGNATURE:

Date:

APPENDIX C. SIPRNET CHECKLIST

STEP		Yes	No	N/A
1	Does the room meet the criteria for classified processing?			
	If No, has a list of the deficiencies been provided?			
2	Is a Protected Distribution System (PDS) required (in accordance with NSTISSI 7003 and AB 381-14)?			
	If yes contact the USAISEC Information Assurance			
	office and the Army CTTA.			
3	Does the organization have a GSA-approved security container?			
4	Has an IASO been appointed?			
5	Has a DIACAP go-by been provided to the IASO?			
6	Has an IATO been submitted and approved?			
7				
/	Has a final inspection been conducted after the COMSEC			
8	Has a final DIACAP been prepared and submitted?			
0	This a final Differ a been prepared and submitted.			
9	Is the system approved for connection to the SIPRNET?			
10	Has the secure Network group provide the IAM a final copy of			
	their checklist?			
11	Has the COMSEC Custodian provided the IAM his final copy of			
	his checklist?			
10	Equipment list answide d?			
12	Equipment list provided?			
13	COMSEC Custodian Notified of New Key Requirement?			
15		<u> </u>	+	
14	IAM Notified of Installation Completion?			
	······································	1	1	
15	TIER II Notified to setup profiles?			
Protected Distribution System (PDS)

Contact the Information Assurance office for a checklist. This checklist is designed to assist personnel in the process of obtaining a PDS.

APPENDIX D. Information Assurance Manager (IAM) Draft Certification Memorandum

IMSE-RED-IMOS

MEMORANDUM FOR SIPRNET PROGRAM MANAGER

SUBJECT: SIPRNET Certification Memorandum

1. The "organization name" SIPRNET connection meets all of the required security regulatory requirements and is authorized to be connected to the Garrison SIPRNET network.

Information Assurance Manager

APPENDIX E. IATO and DIACAP

Below is an example of an IATO. The go-by for the DIACAP can be acquired by contacting the USAISEC Information Assurance Office.

MEMORANDUM FOR:

SUBJECT: Request for ## Days Interim Authority to Operate (IATO) classification, System for organization.

1. Request your office allow us to operate the computers referenced in the subject line, which are located where, in classification for ## days pending processing of version 1.0 of DIACAP package entitled: Title.

- 2. Justification for IATO:
- 3. Point of contact for this action is Name, office symbol, phone and e-mail address and IASO.

SIGNATURE BLOCK

(Include a copy of the IASO certificate)

APPENDIX F. Fort Covert Acceptable Use Policy

Below is the Garrison Acceptable Use Policy (AUP.)

TO: All Fort Covert SIPRNET Users

SUBJECT: Acceptable Use Policy (AUP)

POLICY: This policy outlines the acceptable use of Fort Covert SIPRNET computer equipment and information systems. This AUP sets forth the principles that govern the use of Fort Covert SIPRNET computers and information systems (IS).

PURPOSE: These principles are in place to protect the employees and Fort Covert from inappropriate or illegal activities. These activities expose the organization to risks including virus attacks, compromises of the network systems and services, and legal issues.

EXPLANATION OF TERMS:

- a. Acceptable Use Policy (AUP)
- b. Information Systems (IS)
- c. Campus Area Network (CAN)
- d. Secure Internet Protocol Network (SIPRNET)
- e. Network Time Protocol (NTP)
- f. System Administrator (SA)

APPLICABILITY: This policy applies to all Fort Covert SIPRNET employees (core or matrix), contractors, and others who have access to Fort Covert SIPRNET IS.

RESPONSIBILITIES AND PROCEDURES:

a. The Information Assurance Manager (IAM) will ensure the development of computer use policies that are cognizant of Department of the Army policies.

b. The IAM will develop and maintain a system to track and monitor the signing of the AUP by all Fort Covert SIPRNET personnel.

c. Users of Fort Covert SIPRNET will read and sign the AUP upon assignment of a SIPRNET account and annually thereafter.

d. The SIPRNET SA will document and maintain a record copy of each signed AUP.

e. The IAM will develop and update the AUP.

f. A copy of the AUP policy will be provided to each employee requesting access to Fort Covert SIPRNET.

g. The AUP will be updated/re-signed annually as part of Fort Covert's IA awareness briefing.

REFERENCES:

- a. Army Regulation (AR) 25-1, Information Management, 30 June 2004.
- b. Army Regulation 25-2, Army Information Assurance (IA), 14 November 2003.
- c. Garrison Policy 25-2, Internet Use Policy, 24 February 2005.
- d. Joint Ethics Regulation, Section 2-301, and Department of Defense Directive 5500.7-R.
- e. Department of Defense Directive 8500.1, Information Assurance, 24 October 2002.

f. Department of Defense Directive 8500.2, Information Assurance Implementation, 6 February 2003.

Fort Covert's SIPRNET Information Systems (IS) Acceptable Use Policy (AUP)

1. Understanding. I understand that I have the primary responsibility to safeguard the Fort Covert's SIPRNET from unauthorized users or inadvertent modifications, disclosures, destruction, and denial of service.

2. ACCESS. Access to the Fort Covert SIPRNET is granted to authorized users only whose access is limited to specific defined, documented, and approved applications and levels of access rights and privileges.

3. REVOCABILITY. Access to the Fort Covert SIPRNET resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified Information Processing. The Fort Covert Classified Local Area Network (CLAN) is the primary IS used for processing classified information. It is a U.S. only system and is accredited and certified to process up to and including SECRET collateral information. Information above the SECRET level will not be processed on the Fort Covert CLAN network. Information processed on the CLAN is routed on the SIPRNET to provide secure e-mail to external DOD organizations through e-mail. Access to the Fort Covert classified IS is limited to users with a bona fide need for classified processing.

5. MINIMUM SECURITY RULES AND REQUIREMENTS. I certify that:

a. I have processed through my respective security office to verify my personal security clearance and to validate that my clearance is commensurate with the level of information to which access is requested.

b. I have completed the Information Assurance (IA) awareness training. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords to protect my workstation and applications. The password is classified and I will protect it as such. I will not share my logon and password.

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software on a government-owned system.

e. I will not attempt to access or process data exceeding the authorized IS classification level to which I have been granted access.

f. I will not alter, change, configure, or modify the IS to which I have been granted access, unless specifically authorized through administrative privileges for a laptop or desktop.

g. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

h. I will safeguard and mark media storage devices (diskettes, CDs, flash drives) with the appropriate classification level labels. These labels are provided by the project office security manager.

i. I will ensure that workstations, laptops, and other government furnished IS hardware are marked with the appropriate security labels. These labels are provided by the project office security manager.

j. Maintenance on Fort Covert's SIPRNET IS will be performed by SIPRNET System Administrators only.

k. I will log off and shut down my computer when away from the workstation.

1. I will immediately report any suspicious output, files, shortcuts, suspected viruses, or system problems to the Fort Covert Help Desk, xxx-xxxx and cease all activities on the system.

m. I understand that each workstation and laptop is the property of the U.S. Government and is provided to me for official and authorized uses. I further understand that this equipment is subject to security monitoring.

n. I understand that I do not have a recognized expectation of privacy in official data on the Fort Covert's SIPRNET IS and that I may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

o. I understand that the monitoring of the Fort Covert's SIPRNET IS will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

6. Acknowledgment. I have read the above requirements regarding use of Fort Covert SIPRNET access systems.

Last Name, First Name MI

Rank/Grade

Office Symbol

APPENDIX G. DIAL-UP ACCOUNT

Procedures for SIPRNET Dial-Up Account:

a. If you require a dial-up SIPRNET account, you DO NOT need to go through your DOIM, but you will need to register through your IASO. He/she will sign off on your security measures and validate your requirement.

b. To begin the process, go to the SIPRNET website: http://ssc.smil.mil, and download two SIPRNET registration forms:

1. SIPRNET Registration Template (Dial-In Access Authorization)

2. User Access Request and Responsibility Statement FH Form 380-23-R-E. Point of contact information is also available on the NIPRNET (for SIPRNET registration) at the DOD Network Information Center (NIC) website.

http://www.nic.mil (Requires CAC login to website.)

c. Mandatory fields on the SIPRNET Registration template must be completed or the system will reject the submission. They are lines: U2A-U2E, U3A-U3G, U4A-B, U4E, U5B, U7A-I. The data is typed to the right of the colon in each field.

d. Please ensure that lines U7A-B are EXACT. The COMSEC Account Number and AUTODIN PLA or the command DMS address, and delivery address can be obtained from your COMSEC CUSTODIAN.

e. You will receive a COMM Server card that contains your user ID and password via Certified Registered mail through the USPS. Your COMSEC key will arrive via FedEx from your COMSEC custodian.

f. It is imperative that a complete and accurate street mailing address is provided for the COMSEC Account Information as FedEx only delivers to street addresses. OCONUS COMSEC keys are sent to the COMSEC custodian via registered mail.

g. Please do not enter U6A-E. NETCOM's SIPRNET Dial-in account office will do that for you. Make sure to include U4C, individual customer's DSN phone number, U4H: alternate DSN phone number (security officer), U5A: SIPRNET e-mail address (if one exists), and U5B: unclassified e-mail address.

h. Fill out with appropriate signatures and fax it to: DSN 821-9427 or (520) 533-9427, attn: Lonnie Perry; or by e-mail: Lonnie.Perry@NETCOM.army.mil (for information/confirmation) or alternately: fax: DSN 879-0766 or (520) 538-0766, attn: Pat Unger e-mail: Patrick.Unger@NETCOM.army.mil.

i. The customer currently pays for services. NETCOM will require a funding POC in order to obtain funding from your organization. Rates are \$50.00 for activation and \$27.00 per month for each card.

j. The customer will supply the terminating equipment, which at this point is a STUIII 1910.

k. An alternative way to obtain a SIPRNET e-mail account is to register with the AKO SIPRNET site, URL-http://www.us.army.smil.mil. This site will provide validated users with SIPRNET e-mail access.

1. POC at NETCOM for assistance is: Patrick.Unger@NETCOM.army.mil

APPENDIX H. SAMPLE SIPRNET PDS SPECIFICATION FOR BRAC/MCA CONSTRUCTION

A sample SIPRNET PDS Specification for BRAC/MCA Construction follows.

PART 1 GENERAL

1.1 CONDITIONS AND REQUIREMENTS

Equipment and materials shall be installed in a neat and workmanlike manner. Methods of construction that are not specifically described or indicated in the Contract shall be subject to the control and approval of the Contracting Officer's Representative (COR). Equipment and materials shall be of the quality and manufacture indicated. The equipment specified is based upon the acceptable manufacturers listed. Where "approved equal" is stated, equipment shall be equivalent in every way to that of the equipment specified and subject to approval. It is the responsibility of the Contractor to prove the submitted product is "equal" to that product which is specified including certification letters and USACTTA approval. Contractor shall notify the COR if they cannot install SIPRNET PDS that complies with this section and references.

1.2 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL SECURITY AGENCY (NSA) NSTISSI 7003 (13 December 1996) Protective Distribution Systems (PDS) NSTISSAM TEMPEST 2/95 (12 December 1995) RED/BLACK Installation Guidance NSTISSAM TEMPEST 2/95A (3 February 2000) Amendment to Advisory Memorandum TEMPEST 2/95 RED/BLACK Installation Guidance

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-569-B (2004) Commercial Building Standards for Telecommunications Pathways and Spaces

USAISEC

SIPRNET Technical Implementation Criteria (STIC)

1.3 SUBMITTALS

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. The following shall be submitted in accordance with Section

01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

PDS Layout Drawings

Include separate plans, elevations, sections, details, and attachments to other work. PDS plan shall indicate PDS carrier route, PDS carrier mounting height AFF, equipment enclosure, pull-box, and secure user drop box locations. PDS plan shall be submitted prior to the completion of the 100% design review to the installation Network Enterprise Center (NEC) or G6 for approval by the Central TEMPEST Technical Authority (CTTA) and the installation Designated Approval Authority (DAA).

H-2

SD-03 Product Data PDS Hardened Carrier Submit Manufacturer's descriptive data.

SD-04 Samples

Surface-Mounted Secure Raceway

Submit three 6-inch lengths of exposed type PDS carrier surface-mounted secure raceway material, including component samples from the manufacturer, and list of material (LOM) to the NEC/G6. Show finishes available (if applicable).

Surface-Mounted Conduit

Submit three 6-inch lengths of PDS carrier conduit material, including component (enclosures, fittings, condulette, etc.) samples and list of materials (LOM) to the NEC/G6.

User Drop Boxes, Pull Boxes, and Enclosures Submit Manufacturer's descriptive data.

1.4 QUALITY ASSURANCE

PDS QA inspections must be completed by NEC personal in 3 phases

1nitial inspection, pre-installation survey to verify PDS pathway routes

- 2. 50% inspection, prior to cable being installed into the PDS
- 3. Final inspection, after cable and epoxy are installed but prior to building turnover

1.4.1 Manufacturer Qualifications

Firms regularly engaged in manufacture of secure raceway systems, boxes, and fittings of the types and sizes required, whose products have been in satisfactory use in similar service for not less than 3 years. Provide fittings and boxes produced by a manufacturer listed in this Section.

1.4.2 Equipment

PDS Carrier shall meet or exceed guidelines as defined by NSTISSI 7003 for a hardened carrier and shall be approved for use by DHS, U.S. Army, U.S. Marine Corps, U.S. Navy, and U.S. Air Force.

1.5 DELIVERY, STORAGE AND HANDLING

1.5.1 Deliver secure raceways, conduit, and components in factory labeled packages.

1.5.2 Store and handle in strict compliance with manufacturer's written instructions and recommendations.

1.5.3 Protect from damage due to weather, excessive temperature, and construction operations.

PART 2 PRODUCTS

2.1 ACCEPTABLE MANUFACTURER

2.1.1 SECURE RACEWAY PDS CARRIER

Provide secure raceway and components manufactured from ferrous material as manufactured by Holocom Networks, Wiremold Legrand Data Fence Secure Raceway, or other US Army CTTA approved equivalent. Installation materials shall be free of any rust, dents, scratches, or manufacturing flaws.

2.1.2 EMT CONDUIT PDS CARRIER

Provide electrical metallic tubing, including fittings, couplers, and connectors, manufactured from ferrous material that meets ANSI C80.3 Electrical Metallic Tubing.

2.1.3 SECURE USER DROP BOX

Provide secure user drop boxes and components as manufactured by Holocom Networks, Wiremold Legrand Data Fence Secure Raceway, or other US Army CTTA approved equivalent.

2.2 PDS CARRIER CONFIGURATION

Secure Raceway carrier system shall be used in office environments, for SIPRNET PDS, unless the installation NEC/G6/G6specifically specifies a Conduit Carrier system. Conduit carrier may be used in Non-office environments, such as hangars, maintenance facilities, warehouse, BCTC, etc.

2.2.1 SECURE RACEWAY CARRIER

a. PDS carrier that is comprised of Secure Raceway systems shall be:

square or rectangular design with removable covers or solid construction,

2 inch x 2 inch raceway; or 2 inch x 4 inch raceway for horizontal backbone;

1 inch x 1 inch or 1/2 inch x 1 inch raceway for vertical raceway to user drops from horizontal backbone;

2 inch x 2 inch raceway or 2 inch EMT conduit for vertical riser runs in between floors;

constructed of ferrous material ducting or raceway;

Utilize elbows, couplings, and connectors of the same type of material.

b. Secure Raceways shall be securely mounted to wall partitions using 1-inch standoff mounting brackets or spacers. At no time will the secure raceways be mounted flush with the wall partition; however, in special circumstances this standoff may be exceeded with prior NEC/G6 approval.

c. Secure Raceway TOP CAP shall not exceed 1/4 inch play within the entire length of the span between locking access points.

d. All interfaces shall be physically inspected to ensure that they are tight and cannot turn.

e. Lock covers shall be physically inspected to ensure that the lock cap is properly seated inside the locking mechanism.

f. Thru-walls kits shall be used when the Secure Raceway passes through wall partitions or floors.

g. Fittings shall include flat, internal, and external elbows; tees; couplings for joining raceway sections; cable retention clips; blank end fittings; and device mounting brackets or plates as applicable. Provide full capacity corner elbows and fittings to maintain a controlled 2-inch cable bend radius that meets TIA-569-B standards.

h. Cable fill in horizontal runs shall not exceed 70% of secure raceway capacity. TIA-569B cable fill standards do not apply.

i. Additional pull points shall be provided IAW the manufacturer's instructions.

j. For Holocom Networks Secure Raceway, installation personnel shall be certified by the manufacturer.

k. For Wiremold Legrand Data Fence Secure Raceway Systems, installation personnel shall be familiar with manufacturer's installation instructions.

2.2.2 CONDUIT CARRIER

a. PDS carrier that is comprised of EMT conduit shall be 1 inch, 2 inch, 3 inch, or 4-inch EMT conduit for horizontal backbone or vertical riser runs; 3/4-inch or 1-inch EMT conduit shall be used for vertical runs from horizontal runs to secure user drop box.

b. All couplers, connectors, condulettes, and fittings shall be constructed of the same type of ferrous metallic material as the EMT conduit.

c. PDS conduit carrier shall be surface-mounted on interior walls using 1/2-inch or 1-inch standoff mounting brackets.

d. PDS conduit carrier fittings and components include LL, LB, and LR elbows; tees; condulette; conduit couplings; box connectors; device mounting brackets or plates as applicable. Provide full capacity corner elbows and fittings to maintain a controlled 2-inch cable bend radius that meets TIA-569-B standards.

Note: condulettes do not provide a 2" bend radius except in larger sizes and listed as Mogul Pulling Elbows.

e. EMT Conduit Compression fittings shall be used to connect EMT conduit carrier sections and components together. Do not use set screw connectors or set screw couplers to connect EMT conduit sections together.

f. Cable fills in horizontal runs shall not exceed 60% of PDS conduit capacity. TIA-569B cable fill standards do not apply.

g. A Pull point with a pull string between every pair of adjacent access/pull locations is required for every 180 degree bends in EMT conduit carrier.

h. All fittings, couplings, nipples, and connectors shall be manufactured from ferrous material.

i. Pull string shall be left in place throughout the conduit carrier, even after cable is pulled, in each horizontal and vertical run.

j. Pull boxes shall be sized according to the size of the conduit, not the number of cables or conduits that enter/exit the pull box. National Electric Code conduit fill standards do not apply.

2.2.3 PDS CARRIER ROUTING

a. Design the PDS carrier route in a tree type fashion. Start at the SIPRNET TR with a single raceway or conduit sized accordingly (cable fill rate shall not to exceed 70% for secure raceway and 60% for EMT conduit) to contain CAT6 UTP cable runs. Extend the PDS carrier from the PDS

horizontal backbone throughout the facility to areas where SIPRNET access will be provided. Branch off the PDS backbone with a horizontal run to an area where Secure User Drop Boxes are located using vertical carrier runs from the horizontal run. TIA-569B change in direction standard does not apply.

b. Use a distributed topology when designing the PDS carrier. Consider locating a small network switch in UAA or CAA spaces (i.e. SCIF, NOC/BOC, etc.) with high concentration of users in an approved equipment enclosure. Where possible, increase the capacity of the network switch to provide service to adjacent spaces.

c. Route the PDS carrier so that it does not cross or interfere with the use or maintenance of windows, doorways, ceiling light, air handler, or fire alert or suppression systems n no case shall the PDS carrier be installed in dead space areas, outside of central office environment (example: closets, bathroom, storage rooms, basements, etc.)

d. Bend (saddle or offset) conduit to follow wall contours and route around wall obstacles (columns, pipes, etc.).

e. Offsets shall be used to route secure raceway systems around columns and other wall partition obstacles.

f. Route PDS carrier so that it is surface-mounted on interior wall partitions unless approved by the installation NEC/G6.

g. Route PDS carrier to maximized cable fills in horizontal runs and reduce the number of horizontal runs within the same space.

h. PDS carrier shall not be mounted to the ceiling structure unless authorized by the NEC/G6.

k. A minimum separation of 6-inches is required between the PDS carrier and water pipes, electrical wires, electrical pipes, plumbing, air conditioning, flues, steam or hot water pipes.

2.2.4 MOUNTING

a. PDS carrier shall be surface-mounted to a wall partition three times for every 10ft of PDS or every five (5) feet and within 1.5 inches of a section or component connection.

b. Where wall mounting is unavailable use appropriately sized all thread rods to mount PDS carrier to ceiling structure, overlap all thread with 1/2 inch conduit, painted white and installed with washers on top of conduit to provide structural stability and improve aesthetics of installation.

c. PDS carrier shall not be mounted to ATC framework.

d. Fasten PDS carrier and component items to permanent building wall partitions using the appropriate anchor or fastener for the wall partition type.

e. PDS carrier shall be level and plumb along its route.

f. Mount PDS carrier with center line of PDS 3 to 8 inches below final ceiling level in spaces with finished ceilings to allow 360-degree visual inspection.

g. Use Arlington Quick Latch Hangers (or equivalent) to mount PDS Conduit carrier to wall partition.

h. UNISTRUT shall not be used to mount secure raceway or conduit to wall partitions.

2.2.5 SECURE USER DROP BOX

a. Secure User Drop Box shall be at least 7-inch high by 6-inch wide by 4-inch deep, tamperresistant design constructed from 16-gauge steel with welded internal hinges. Exterior hinges are not acceptable.

b. User Drop Boxes shall have a single door with a built-in steel hasp that accepts a Sargent & Greenleaf 8077AD padlock.

c. User Drop Boxes shall be surface-mounted on the wall partition 48 inches to 60 inches above final floor line, unless otherwise specified by NEC/G6, depending on room furniture height and layout.

d. User Drop Boxes shall be fastened to the wall partition using screws or bolts appropriate for the wall partition type.

e. Up to 6 cable connections may be terminated within the drop box on a single gang faceplate as long as it is within 15 feet of the classified workstations and/or printers are located in the same room.

f. User Drop boxes shall not have pre-punched knockouts.

Indicate User Drop Box locations on shop and as-built drawings.

2.2.6 ENCLOSURES

a. Equipment and Pull-box enclosures shall be constructed from 16-gauge steel; have a single door with a built-in steel hasp or multi-point security hasp that accepts a Sargent & Greenleaf 8077AD padlock; and a tamper-resistant design with welded internal hinges.

b. Enclosures shall be fastened to the wall partition using screws or bolts appropriate for the wall partition type.

c. Enclosures shall not have pre-punched knockouts.

Indicate enclosure type (equipment or pull-box) on shop and as-built drawings.

2.2.7 COMMUNICATION DEVICES

Enclosures shall accommodate a complete line of open connectivity outlets and modular inserts for Category 6 UTP or STP cable, fiber optic, and other cabling types with matching faceplates and bezels to facilitate mounting. STP cabling shall use shielded connectors, jacks, and patch panels.

PART 3 EXECUTION

3.1 EXAMINATION

Examine the route and mounting locations of the raceways, boxes, distribution systems, supporting structure and accessories, to determine if conditions exist that will inhibit or prevent proper PDS installation. Notify the Contracting Officer's Representative (COR) in writing of conditions detrimental to proper completion of the work. Do not proceed with work until unsatisfactory conditions have been corrected.

3.2 INSTALLATION

a. Strictly comply with manufacturer's installation instructions and recommendations and approved shop drawings.

b. Coordinate installation with adjacent work to ensure proper clearances and compliance with project site NEC/G6, DAA, and USACTTA.

H-7

c. The PDS Carrier shall be surface-mounted to wall partitions as specified in 2.2.1 or 2.2.2 and 2.2.4.

d. The top edge of the carrier shall be horizontally level a minimum of 3-inches below the suspended ceiling line or the true ceiling line, whichever is lower.

e. The PDS carrier shall be installed to permit visual inspections of its entire run.

f. The PDS carrier shall not block doorways or access to emergency exits; shall not inhibit the operation of windows; and shall not be run across windows, air vents, water sprinklers, lights or air flow intakes.

g. The PDS carrier shall not be painted or covered with wallpaper or other covering unless the paint is applied by the carrier manufacturer.

3.2.1 MECHANICAL SECURITY

a. A continuous bead of two-part epoxy shall be applied at all component, coupling, and fitting connection joints of an EMT conduit PDS carrier system.

b. Pull box covers shall be sealed to the pull boxes around the mating surfaces after installation with a continuous bead of two-part epoxy if they cannot be secured with GSA-approved changeable combination padlock.

c. Obtain site specific epoxy standards from installation NEC/G6.

3.2.2 CARRIER SUPPORT

Carrier shall be supported by mounting brackets at intervals not to exceed 5 feet or in accordance with manufacturer's installation sheets.

3.2.3 ACCESSORIES

Provide accessories as required for a complete installation to include Sargent & Greenleaf 8077AD changeable combination padlock for every user drop box, secure cable entry boxes, and all junction boxes which requires a lock.

3.3 CLEANING AND PROTECTION

Clean exposed surfaces using non-abrasive materials and methods recommended by manufacturer. Protect raceways and boxes until acceptance.

3.4 PDS APPROVAL REQUEST

a. Coordinate with the installation NEC/G6 to obtain PDS installation approval from the USACTTA and installation DAA.

b. Provide PDS carrier shop drawings, LOM, and any other documentation required to the installation NEC/G6 90-days prior to the installation of PDS carrier.

c. PDS design approval must be obtained prior to installation.

APPENDIX I. SIPRNET GROSS COST ESTIMATION TOOL

An example of the Cost Estimation Tool results is shown below. The Tools (Microsoft Excel) are available on a CD provided by USAISEC and at the AKO website.

Other Costs and Labor SIPRNET Estimator							
Item Description	Configuration	Unit Cost	Qty	Equipment Costs	Install / Labor Cost	Procurement/ Travel Cost	Total Cost
Site Preparation for Secure Room: Door CDX09 Lock Power Upgrades Other Site Prep Intrusion Detection System (for the room) Core Drill	Door must be solid wood or steel. Fill in Unit Cost. Lock must meet Fed Spec FF-L-2740A. Fill in Unit Cost. This will be a site responsibility. Fill in Unit Cost. HVAC, Windows, Walls, Ceiling, etc. Fill in Unit Cost. This will be a site responsibility. Fill in Unit Cost. Core drills will be accomplished as identified in survey. Fill in Unit Cost.	\$0.00 \$2,200.00 \$0.00 \$0.00 \$0.00 \$0.00					
Indirect Costs: Site Survey (per person basis, except rental car) - Manhours - Airfare - Lodging/Meals - Rental Car Development of TACE Freight and Shipping Costs	Typical survey is one week (48 hours@\$78/hour) Estimated for average airfare (\$800/roundtrip) Estimated for average per diem (\$150/day@6 days) One car per two people Two weeks for one person (80 hours@\$75/hour) Estimated cost	\$5,944.00 \$3,744.00 \$900.00 \$500.00 \$6,000.00 \$1,000.00	1 1 1 1 1	\$1,000	\$3,744 \$6,000	\$800 \$900 \$500	\$3,74 \$80 \$90 \$50 \$6,00 \$1,00
Installation Costs (per person basis, except rental) - Manhours - Airfare - Lodging/Meals - Rental Car - Cargo Van Sefe Marger	Travel time only - Installation time shown with materials Estimated for average airfare (\$800/roundtrip) Estimated for average per diem (\$150/day@12 days) One car per two people (\$500/week@2 weeks) Required for moving equipment	\$26,300.00 \$1,200.00 \$800.00 \$1,800.00 \$1,000.00 \$200.00	6 6 3 1		\$7,200	\$4,800 \$10,800 \$3,000 \$500	\$7,20 \$4,80 \$10,80 \$3,00 \$50
Accreditation - develop documentation for DOIM - Complete set of docs (never done before) - Existing accreditation, update only Additional tams (added by site or angineer)	Paperwork completed only on SIPRNET additions Paperwork completed only on SIPRNET additions Can enter unit cost, quantity, install/labor cost, and	\$200.00 \$17,000.00 \$9,000.00	1		\$9,000	\$1,200	\$9,00
1. 2. 3. 4. 5. 6. 7. 8. 9.	procurement/travel costs.						
		Page 2 Total		\$1,000	\$27,144	\$22,500	\$50,64

This page intentionally left blank.

APPENDIX J. SAMPLE IPS CONTAINERS WITH MOVABLE RACKS

A sample IPS containers with movable racks follows.



NOTES

- 1 IPS shown is the Hamilton BW-2717 model.
- 2 The IPS requires certain minimum clearances around it in order to function properly, and to allow for ease of inspection. All clearance dimensions are from the surface of the IPS.
- 3 The IPS weights approximately 950 lbs empty. The four support legs on the IPS provide only 81 in² (0.5625 ft²) of floor contact area. Approximate floor loading is thus about 1,690 lbs/ft², which is above the GSA standard of 250 lbs/ft². Use of the 29"x48" floor plate provides 9.66 ft², reducing the floor loading to approximately 100 lb/ft²
- 4 The rack may be rolled out, clearing the IPS door, with the door open 100 degrees, which requires 5" of clearance from the wall.

Minimum	Clearance	Dimensions
---------	-----------	------------

Front	34"	for rack rails & frame
Hinge Side	5"	to open door for rack rollout
	25"	to fully open door
Rear	9"	for PDS box
Left Side	3 1/2"	for ear muff
Room Door	29"	to allow IPS to enter

Figure J-1. Hamilton IPS Clearance Requirements







NOTES

- 1 IPS shown is the Trusted Systems TSM281WFC model.
- 2 The IPS requires certain minimum clearances around it in order to function properly, and to allow for ease of inspection. All clearance dimensions are from the surface of the IPS.
- 3 Rack may be rolled out, clearing the IPS door, with the door open 90 degrees, which requires 3 1/ 2" clearance. The tracks for the rack must be stored separately when not in use. The rails are 50" long and 3 1/2" wide.

Minimum Clearance Dimensions

Front	43"	for rack rails & frame
Hinge Side	3 1/2"	for air flow
	28 1/4"	to fully open door
	5 1/2"	to open PDS box door
Rear	6 1/2"	for PDS box
Left Side	3 1/2"	for air flow
Room Door	30"	to allow IPS to enter

Figure J-3. Trusted Systems IPS Clearance Requirements



Figure J-4. Trusted Systems IPS Dimensions

J-5 FOR OFFICIAL USE ONLY

This page intentionally left blank.

APPENDIX K. MCA/BCA FUNDING BREAKOUT



K-1 FOR OFFICIAL USE ONLY

This page intentionally left blank.

GLOSSARY. ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

AC	alternating current
ACL	access control list
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APL	Approved Products List
AR	Army Regulation
ATC	Authority To Connect
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
AWCF	Army Working Capital Funds
BBP	Best Business Practices
BCT	Brigade Combat Team
BRAC	Base Realignment and Closure
~	
C	Classified
C&A	Certification and Accreditation
C2	command and control
C4IM	command, control, communications, computers, and information
	management
CA	Certification Authority
CAA	controlled access area
CAC	Common Access Card
CAD	computer-aided design
CAN	campus area network
CAO	Connection Approval Office
CAP	Connection Approval Process
CCI	Controlled Cryptographic Item
CD	compact disk
CDS	Cross Domain Solutions
CE	Embedded Compact
CENTCOM	Central Command
CERDEC	Communications-Electronics Research Development and Engineering Center
CI	Cryptographic Item
CIK	Crypto Ignition Key
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
cm	centimeter
CMOD	Cryptographic mModule
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CNSSP	CNSS Policy
CODEC	coder/decoder

Glossary-1

COMSEC	communications security
CONUS	Continental Unted States
CSLA	Communications Security Logistics Agency
CTTA	Certified TEMPEST Technical Authority
DA	Department of the Army
DAA	Designated Approving Authority
dB	decibel
DFAS	Defense Finance and Accounting Service
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DNS	Domain Name Services
DOD	Department of Defense
DPW	Directorate of Public Works
DRSN	Defense Red Switch Network
DS3	Digital Signal Level 3
DSN	Defense Switched Network
DTD	data transfer device
DVD	digital video disk
DVS-G	DISN Video Sevices-Global
EIA	Electronic Inductrics Allience
EIA	Electronic industries Alliance
EKMS	Electronic Key Management System
EMOD	Ethernet Module
EMI	electrical metallic tubing
EUB	end user building
F	Fahrenheit
FDED	Fort Detrick Engineering Directorate
FOUO	For Official Use Only
FTR	Field Tamper Recover
FVS	Firefly Vector Set
FY	Fiscal Year
Gbps	gigabit per second
GIG	Global Information Grid
GSA	General Services Administration
GSM	Global System for Mobile
HAIPE	High Assurance Internet Protocol Encryptor
HAIPE IS	HAIPE Interoperability Specification
HAIPIS	High Assurance Internet Protocol Interoperability Standard
	ingli i issurance memer i rotocor meroperatinty standard

Glossary-2

I3MP	Installation Information Infrastructure Modernization Program
IA	information assurance
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IAVA	IA Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	in accordance with
ICAN	installation campus area network
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IME	Individual Mobile Encryptor
IMO	Information Management Officer
IMUX	inverse multiplexer
INE	In-Line Network Encryptor
IP	Internet Protocol
IPS	information processing system
IS	information system
ISD	Information Service Division
ISDN	Integrated Services Digital Network
ISSP	Information Systems Security Program
IT	information technology
Kbps	kilobits per second
km	kilometer
LAN	local area network
lb	pound
lbs/sq ft	pounds per square foot
LC	Lucent Connector
LCA	limited control area
LCD	liquid crystal display
LEF	Link Encryption Family
LOAC	Law of Armed Conflict
LOM	list of materials
LVDS	Low Voltage Differential Signaling
ΝΛΑΝΤ	matropolitan area natival
MAN	metropontan area network
MOA	Military Construction Array
MCA	Multi Domain Security Solutions
MD22	Multi-Domain Security Solutions
	Military Handbook
MIL-TUDK	Military Standard
	Multi Loval Soourity
MTDE	Maan Time Detween Feilure
MIRF	wiean Time Between Failure

Glossary-3

MTTR	Mean Time To Repair
NEC NEMA NETCOM NFPA NIDS NIPRNET NIPS NNX NSA NSI NSTISSAM NSTISSAM	Network Enterprise Center National Electrical Manufacturers Association Network Enterprise Technology Command National Fire Protection Association network intrusion detection system Unclassified but Sensitive Internet Protocol Router Network network intrusion prevention system Network Numbering Exchange National Security Agency National Security Information National Security Telecommunications and Information Systems Security Advisory Memorandum National Security Telecommunications and Information Systems Security Committee
O&M	operations and maintenance
OC	Optical Carrier
OCONUS	Outside Continental United States
OMA	O&M, Army
OPA	Other Procurement, Army
OS	operating system
OSI	Open Systems Interconnection
OTAR	Over The Air Rekey
PC	personal computer
PCMCIA	Personal Computer Memory Card International Association
PDS	protective distribution system
PKE	Public Key Encryption
PoE	Power over Ethernet
PoP	point of presence
PPK	Pre-Placed Key
PSTN	Public Switched Telephone Network
QoS	quality of service
RDP	Remote Desktop Protocol
RF	radio frequency
RMOD	Radio Module
RTS	Real Time Services
RU	rack unit
SCIP	Secure Communications Interoperability Protocol
SDD	Secure Data Device

Glossary-4

SFP	small form factor pluggable
SIPRNET	Secret Internet Protocol Router Network
SKL	Simple Key Loader
SMA	Sub-Miniature version A
SNMPv3	Simple Network Management Protocol version 3
SOCOM	Special Operations Command
SONET	Synchronous Optical Networking
SOP	Standing Operating Procedure
SSO	Site Security Officer
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
STU	Secure Telephone Unit
SWA	South West Asia
SWLAN	secure local area network
SWT	Sectera Wireline Terminal
TA/CF	technical analysis and cost estimate
TACLANE	Tactical Local Area Network Encryptor
TR	Technical Bulletin
TCO	Total Cost of Ownership
ТСР	Transmission Control Protocol
TEK	Transmission Encryption Key
TIA	Telecommunications Industry Association
TIC	Technology Integration Center
ne	reemonogy megration center
U	Unclassified
UAA	uncontrolled access area
UDB	user drop box
UDP	User Datagram Protocol
UPS	uninterruptible power supply
URL	Uniform Resource Locator
USAISEC	U.S. Army Information Systems Engineering Command
USAR	U.S. Army Reserve
USB	universal serial bus
VAC	volts alternating current
VDC	volts direct current
VLAN	virtual local area network
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPN	virtual private network
VTC	video teleconferencing
VVoIP	Voice and Video over Internet Protocol

Glossary-5 FOR OFFICIAL USE ONLY

W	watt
WAN	wide area network
WAP	wireless access point
WIDS	wireless intrusion detection system
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless local area network
WPA2	Wireless Protected Access 2

XFP small form factor pluggable

Glossary-6 FOR OFFICIAL USE ONLY

ATTACHMENT 1. DRAFT MEMORANDUM, ARMY CTTA, SUBJECT: UPDATED INSTALLATION GUIDELINES FOR SECNET 11 LOCAL AREA NETWORKS IN U.S. ARMY FIXED FACILITIES AND SYSTEMS (MMN 20073381)

The Draft Memorandum follows.

Att 1-1 FOR OFFICIAL USE ONLY



UNCLASSIFIED//FOR OFFICIAL USE ONLY

DEPARTMENT OF THE ARMY 310TH MILITARY INTELLIGENCE BATTALION 4552 PIKE ROAD FORT GEORGE G MEADE MD 20755-5995

IAMG-CIC-OP-CTTA

MEMORANDUM FOR USAISEC FDED, 1435 Porter Street, Suite 200, (ATTN: Kim Reed), Fort Detrick, MD 21702.

SUBJECT: Updated Installation Guidelines for SECNET™ 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20073381)

References:

Confidential AR 381-14, 30 September 2002, Technical Counterintelligence (TCI) (U).

 FOUO manual NSTISSAM TEMPEST/2-95 with Amendment A, National Security Agency, 12 December 1995, RED/BLACK Installation Guidance (U).

c. FOUO instruction CNSSI No. 3034, Committee on National Security Systems, April 2004, Operational Security Doctrine for the SECNET™ 11 Wireless Local Area Network Interface Card.

d. Unclassified document, National Security Agency, March 2004, Secure Wireless LAN CONOPS.

e. Unclassified document, Wireless STIG, Department of Defense, 20 February 2007, Wireless Security Technical Implementation Guide, Version 5, Release 1.

f. Unclassified document, Addendum to Wireless ST IG, Department of Defense, 31 October 2005, Secure Wireless Local Area Network Addendum to the Wireless Security Implementation Guide.

g. Unclassified AR 25-2, 14 November 2003, Information Assurance.

h. FOUO memorandum, 310th Military Intelligence Battalion, IAMG-CIC-OP-CTTA, 3 October 2006, subject: Installation Guidance for SECNET™ 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20063433).

 FOUO memorandum, 310th Military Intelligence Battalion, IAMG-CIC-OP-CTTA, undated, subject: Revised Installation Guidelines for SECNET[™] 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20063433).

 (FOUO) This memorandum supersedes the previous memoranda listed as reference 1h and 1i. This update removes the 20 meter control space for the SECNET™ 11. Per verbal discussions between the Army CTTA and the proponent for the DoD Wireless STIG, the 20 meter control space requirement was not valid and is being removed from future revisions of reference 1f.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Att 1-2

UNCLASSIFIED//FOR OFFICIAL USE ONLY

IAMG-CIC-OP-CTTA

SUBJECT: Updated Installation Guidelines for SECNET[™] 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20073381)

3. On 9 April 2007, Mrs. Gina DuBell, Certified TEMPEST Technical Authority (CTTA), set the following installation criteria as the minimum standards for all U.S. Army SECNETTM 11 Wireless Local Area Networks installed in U.S. Army fixed facilities. These minimum standards are derived from the national and DoD level standards in references 1c, 1d, 1e, and 1f. For the purposes of this document, a SECNETTM LAN card installed in a laptop is mobile, unless the laptop is installed in a docking station. When installed in a docking station, the laptop will be treated as a fixed device. All other SECNETTM 11 devices will be treated as fixed devices, unless specific operational policies (see paragraph 3.b.) have been approved by the supporting CTTA.

a. The following minimum standards apply to fixed SECNETTM 11 devices.

 (U//FOUO) Maintain at least 3 meters separation between any fixed SECNET[™] 11 and any RED processor.

 (U//FOUO) Maintain at least 3 meters separation between any fixed SECNET[™] 11 and any other fixed transmitter.

 (U//FOUO) Maintain at least 3 meters separation between any fixed SECNET™ 11 and any other fixed SECNET™ 11.

 (U//FOUO) Maintain at least 1 meter separation between any fixed SECNETTM 11 and any BLACK equipment.

 (U//FOUO) Maintain at least 1 meter separation between any fixed SECNET™ 11 and any BLACK wire lines that exit the inspectable space or are connected to an RF transmitter. (Request inspectable space determination from the supporting CTTA.)

 (U//FOUO) Maintain at least 1 meter separation between any fixed SECNET[™] 11 and any BLACK power lines.

 (U//FOUO) Maintain at least 1 meter separation between any fixed SECNETTM 11 and fortuitous conductors that exit the inspectable space.

b. The following minimum standards apply to mobile SECNET™ 11 devices.

 (U/FOUO) The DAA must ensure an operational policy is in place to remove the mobile SECNET TM 11 devices from the work space at the end of each duty cycle. This policy preserves the mobile characteristics of the device.

2) (U/FOUO) The user must not plug a laptop with a SECNET[™] 11 LAN card installed into any docking station that has not been specifically installed to meet all the SECNET[™] 11 fixed device requirements of paragraph 3a. It would be permissible to install the laptop in any docking station after removing the SECNET[™] 11 LAN card.

 All SECNETTM 11 installations must be approved by the supporting CTTA prior to any implementation, and preferably prior to obligating any funds.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Att 1-3

UNCLASSIFIED//FOR OFFICIAL USE ONLY

IAMG-CIC-OP-CTTA

SUBJECT: Updated Installation Guidelines for SECNET™ 11 Local Area Networks in U.S. Army Fixed Facilities and Systems (MMN 20073381)

5. The introduction of wireless technology into a classified processing area increases the technical threats to the area. Before submitting a proposed installation to the supporting CTTA, the user should ensure that the wireless technology is mission essential, or enhances the mission to the point that the benefits offset the potential threat and cost. The supporting CTTA can be contacted to provide the TEMPEST threats related to a specific facility or system.

6. This memo provides minimum standards. The supporting CTTA may require additional TEMPEST countermeasures based on the threat to a specific facility or system.

 For SCIFs, the supporting CTTA will be the CTTA for the SCIF accrediting agency. For all other Army, Army National Guard, Army Reserve, and DoD contractors doing work for the U.S. Army, the supporting CTTA, and the point of contact for this memo, is Mr. Donald Bell, Technical Operations Officer, at Commercial (301) 677-4440 or DSN 622-4440.

> MICHAEL S. SIMPSON LTC, MI Commanding

Att 1-4 FOR OFFICIAL USE ONLY
ATTACHMENT 2. E-MAIL, 7TH SIGNAL COMMAND, BG NAPPER, SUBJECT: WAIVER FOR USE OF EPOXY ON PDS, 23 OCTOBER 2009

The 7th Signal Command e-mail follows.

Att 2-1 FOR OFFICIAL USE ONLY From: Napper, Jennifer L BG MIL USA NETCOM/9TH SC A 7TH SC Sent: Friday, October 23, 2009 4:43 PM To: BDE 93d DIACAP; 106th Sig Bde - IA; Barrett, Gerald S Mr CIV USA NETCOM/9TH SC A; Houst, Peter J CIV USA NETCOM/9TH SC A; Lyday, Sandra CIV USA NETCOM/9TH SC A 7TH SC; McDonald, Justine E CIV USA NETCOM/9TH SC A 7TH SC; Sheppard, Dennis K Mr CIV USA NETCOM/9TH SC A 7TH SC; Gregory, Josalyn S USA NETCOM/9TH SC A 7TH SC Subject: Waiver for use of Epoxy on PDS

I, the Designated Approval Authority (DAA) for 7th Signal Command (T) ICANs, assume the risk and approve the use of Holocom PDS without the use of Epoxy. This will expedite adjustments to the configuration of the PDS on Installation SIPRNet ICANs. All other stipulations in their original ATOs remain in place.

JENNIFER L. NAPPER Brigadier General, USA Commanding

Situation Summary:

The Protected Distribution System (PDS) installed and maintained for the protection of SIPRNet and Defense Red Switch Network (DRSN) connections consists of a combination of Electrical Metallic Tubing (EMT) and both aluminum and steel raceway manufactured by Holocom. The Holocom system is installed exclusively by Holocom certified technicians to ensure that it is installed according to the manufacturer's specifications, and in accordance with applicable regulations and policy. The Holocom raceway includes the configuration of a Steel Raceway Locking Kit, (See appendix D) which secures the entire raceway through an internal locking mechanism, preventing the system from being opened without considerable destruction of the raceway material and/or probable detection. In addition, the Holocom raceway is installed with a tamper-indicative paint, allowing for quick detection of attempted or actual intrusion/tampering of the system. As stated in NSTISSI 7003: "The emphasis is placed on "detection" of attempted penetration in lieu of "prevention" of penetration." NSTISSI 7003 mandates that for a Hardened Distribution System: "All connectors should be permanently sealed completely around all surfaces (e.g. welding (continuous or track), compression, epoxy, fusion, etc.)" However, NSTISSI 7003 also states: "The decision as to what extent the Guidance is followed ultimately rests with the department or agency Approval Authority." While this requirement is entirely appropriate for PDS installations consisting of EMT due to the lack of built-in locking or

Att 2-2 FOR OFFICIAL USE ONLY

protection mechanism, it prevents the unlocking and opening of the Holocom raceway in order to add to, or change the installation configuration.

Raceway is the preferred installation material on multiple installations due to the fact that units and organizations move and change buildings throughout the deployment/redeployment cycle, requiring considerable additions and/or changes to the PDS configuration. This requirement will increase significantly with the expansion of SIPRNet connectivity to Company-level elements.

If the Holocom PDS Top Caps, Raceway sections and all connections are welded or treated with epoxy, it prevents the opening of the locking kit by the authorized technician to reconfigure the installation without considerable damage to the tamper-indicative paint and component surfaces. This damage thereby prevents the additions and changes required without additional cost and manpower to the government to replace the damaged parts and/or paint. The benefits associated with the easily reconfigurable raceway system far outweigh the benefits of additional sealing measures. As the raceway includes an adequate locking mechanism, layered with the regular inspections of the PDS in the relatively low risk environment of CONUS, it is requested that the DAA approve a waiver allowing for the installation and maintenance of Holocom raceway without permanently sealed or epoxied surfaces on the re-configurable portion of the PDS.

Justine E. McDonald Information Assurance Specialist 7th Signal Command (T), G-3 Information Assurance Fort Gordon, GA 30905 Justine.McDonald@us.army.mil Justine.McDonald@us.army.smil.mil (706) 787-7966 | DSN 773

" The world is governed more by appearances than realities, so that it is fully as necessary to seem to know something as to know it." - Daniel Webster

Classification: UNCLASSIFIED Caveats: FOUO

APMS	Current System Acronym	Installation	ICAN	CCSD	ATO/IATO	EXP Date
DA147011	APG ICAN	Aberdeen Proving Ground	NIPR	737X / 70S1		12/28/2011
DA95900	ARLEN	Adelphi Lab	NIPR	73CA / 7FRE		
DA147100	ANADNET	Anniston	NIPR	7384 / 7AU4		
DA146707	FORT A P HILLAN	AP HIL	NIPR	UTC Off of Belvoir		
DA146334	LAN FT BELVOIR	Belvoir	NIPR	76GL / 73GC/ 76RL		
DA147301	LAN FT BENNING	Benning	NIPR	7209		6/30/2012
DA147312	CAN ET BLISS	BUISS	NIPR	7614 72PB 7568 7V94		8/30/2012
DA146577	ICAN ET BRAGG	Brann	NIPR	79R1 / 733X	IATO	4-Nov-09
DA146905	I AN ET RUCHANAN	Buchanan	NIPR	GIGU	1410	41101-03
DA147098		Campbell	NIPR	78ME / 72VR	IATO	9/25/2009
DA145540	LAN CAPITSIE BARRACKS	Carlisle	NIDR	72DE	1210	3/23/2003
DA147035	LAN ET CARSON	CARSON	NIPR	72FC		
DA156360	TLA- Top Level Architecture	C-TNOSC	NIPR	-2011,1427,71174		
DA 164231	AD CONUS Forest	C-TNOSC	NIPP			
200 200 201		Detrick	NIPR	7441 / 77549	ATO	12/22/2009
DA446993	LAN DETROIT ABSENCE	DETROIT ARSENIAL	NICS	200 26VC 2116U	210	12/2//2009
DA146565		Devens	NICR	3/6/C,/00H	ATO (OD day)	42/42/2000
DA146474	LAN FT DEVENS	Div.	NIDR	74960	ATO (90 089)	12/15/2009
DA146046		Dave Course	NIPR	7400771E3		40/24/2000
LA 140940	LAN FI DROM	Drum	NIPR	7328	IATO	10/21/2009
DA146993	LAN DUGWAY PROVING GROUND	DUGWAY PROVING GROUND	NIPR	75C0,7TMJ	ATO	11/16/2009
DA146326	LAN EUSTIS	Eustis/Story	NIPR	72P1 / 75EE		
DA146354	LAN FT GORDON	Gordon	NIPR	72PG / 7WV4	ATO	9/15/2012
DA146377	LAN FT HAMILTON	Hamiton	NIPR	71PC/7PB4/7W2K		
DA146735	LAN FT HOOD	ноор	NIPR	7365,7EW6,7GW6,7MW6		
DA176080	LAN FT HUACHUCA	HUACHUCA	NIPR	72P7	IATO	11/13/2009
DA184928		HUNTER LIGGETT	NIPR	720L,7RWH,7VGK		6/1/2012
DA146738	LAN FT IRWIN	IBWIN	NIPR	736N,76XC,772M		1/5/2012
DA181969	LAN FT JACKSON	Jackson	NIPR	72PD / 78Q6		
DA168183	LAN FT KNOX	Knox	NIPR	72P8 / 76XD / 77JF		
DA147300	LAN FT LEAVENWORTH	LEAVENWORTH	NIPR	72P9,7YV6		2012
DA145689	LAN FT. LEE	Lee	NIPR	72PA		3/9/2012
DA158801	LAN-FT LEONARDWOOD	LEONARD WOOD	NIPR	72PF,7NW6,7XQ6		
DA168692	FTUCAN-U	LEWIS	NIPR	72R8,7P66	IATO	11/28/2009
DA146885	LAN FORT MCCOY	MCCOY	NIPR	749P		
DA111014	FCCSU	McPherson /Gillem	NIPR	72PZ / 7V32		
DA146468	LAN FT MEADE	Meade	NIPR	737Y		
DA145532	LAN FT MONMOUTH	Monmouth	NIPR	7081 / 73BM	IATO	11/14/2009
DA146325	LAN FT MONROE	Monroe	NIPR	72PC / 77GB		
DA146709	LAN FT MYER	Myer/McNair	NIPR	UTC Off of Belvoir		
DA146447	LAN NATICK	Natick	NIPR	703J		
DA66753		Picatinny Arsenai	NIPR	76VM	IATO	12/12/2009
DA163719	LAN FT POLK	Polk	NIPR	72VQ / 7V44 / 78G6 / 76YM		
DA159429	LAN PRESIDIO OF MONTEREY	PRESIDIO OF MONTEREY	NIPR	72V5,76Y5,7V79,		
DA176112	LAN FT RILEY	RILEY	NIPR	736L,795B,7RW5		3/26/2011
DA158935	LAN RIA	ROCK ISLAND ARSENAL	NIPR	738L,7RF5,7URD	ATO	12/28/2009
DA146752	LAN FT RUCKER	Rucker	NIPR	7Z77 / 72PX		
DA146893	FORT SAM HOUSTON NIPRNET	SAM HOUSTON	NIPB	7846 71DB 751K 7WH2	ATO	11/18/2009
DA146953	LAN FT SILL	SILL	NIPR	72PI 7773 7954		
DA146868	LAN FT STEWART	Stewart/Hunter AAF	NIPR	72VT		
DA184427	7thSieCtr NIPRNet ITS	s-TNOSC	NIPR	705V	ATO	11/25/2011
DA185820	MOTSU NIPRNET LAN	Sunny Point	NIPR	74N9 / 737T / 7REA / 7TXA		
	WVAN	Watervilet Arsenal	NIPR	7FFS / 78SC		
DA146991	I AN WEST POINT	West Point	NIPR	74UU / 7SM4 / 777E		17-Eab-12
DA184051	APG SIPPRIET ICAN	Aberdeen Proving Cround	SIPR	7485		17-760-12
DA00504	ATM	Afface	SIDE	77E3/7T/8		e/se/sees
DA187000	ANAD CIRCUST	Annistan	SIDE	7006		5/23/2009
DA184952			SIPR	IMOONI		
DA193440		Per filli Reliveir	OIPR	INUUM 221.0 (221/8) 22:001 24/50		
DA103110	PIBELVOIR SIPRNET LAN	Devoir Receive	SIPR	Zace / /ZNo/ /3GC/ /W59		a la stance
LIA105/66	SLAN Fort Benning	bening	SIPR	/0/C	ATO	9/14/2012
DA176153	FBSCAN	BLISS	SIPR	75V3,7U04,7Z54,7NUK		9/7/2012
1	XVIII ABN	Bragg	SIPR	7QQA, 7ZS2	ATO	9/27/2009

Att 2-4 FOR OFFICIAL USE ONLY

APMS	Current System Acronym	Installation	ICAN	CCSD	ATO/IATO	EXP Date
		Bragg	SIPR	7PAJ		
DA184697	SICAN FT BRAGG	Bragg	SIPR	75S0 / 796B	ATO	11/1/2009
DA182758		Buchanan	SIPR	G34Y		
DA184989	SLAN FT CAMPBELL	Campbell	SIPR	75R6	ATO	12/21/2009
DA190263	SIPRNET LAN CARLISLE BARRACKS	Carlisie	SIPR	71A9		
DA186154		CARSON	SIPR	2725,75HW		
DA184957	SIPRNET - DTA	DETROIT ARSENAL	SIPR	72RO		
DA184843	FORT DIX SIPR	Dix	SIPR	75JE		
DA192946		Drum	SIPR	27HA / 700H		
DA186100		DUGWAY PROVING GROUND	SIPR	73H3		2010
DA184699		Eustis/Story	SIPR	73VC / 73VE / 703Y		
DA184842	SIPRNET FT GORDON	Gordon	SIPR	7TV2/71A7		
DA187457		HOOD	SIPR	767Q,7P76,7PW5,7QW7	ATO	11/8/2009
DA187451	SIPR FT HUACHUCA	HUACHUCA	SIPR	70NB,76YR,7GY3		
DA184929		HUNTER LIGGETT	SIPR	75JN		
DA184952		IRWIN	SIPR	739E,76CT		
DA184879	SIPR FT JACKSON	Jackson	SIPR	7GT2 / 7ZN4		
DA184885	SLAN FT KNOX	Knox	SIPR	7786 / 76CP		
DA184676	FORT LEAVENWORTH SIPRNET	LEAVENWORTH	SIPR	7JA1	ATO	11/4/2009
DA184024	SLAN FT LEE	Lee	SIPR	719W / 7X9H	ATO	10/24/2009
DA192589		LEONARD WOOD	SIPR	718J	IATO	11/3/2009
DA190202		LEWIS	SIPR	76MZ,7GN5	IATO	2/24/2010
DA184894	SLAN FT MEADE	Meade	SIPR	766N / 770K	IATO	11/7/2009
DA184938	SIPRNET FT. MONMOUTH	Monmouth	SIPR	72DH		
DA184691	IWP FT MONROE SIPRNET	Monroe	SIPR	7184 / 74MU		
DA181953		Natick	SIPR	71CA		
DA176318	LAN PICATINNY ARSENAL	Picatinny Arsenai	SIPR	75R4 / 7W5C		
DA187127		Polk - JRTC	SIPR	23BG / 78F9	IATO	11/24/2009
DA184984	SLAN POM	PRESIDIO OF MONTEREY	SIPR	71A5,76XT		
DA186919	AVN MS CMD REDSTONE	Redistone Arsenal	SIPR	7761 / 7861	ATO	
DA168685	HELP DESK FT RILEY ???	RILEY	SIPR	2721,75W5		
DA184665	SLAN RIA	ROCK ISLAND ARSENAL	SIPR	27FQ,78R5,7P45,7VXJ		
DA184971	FRSCAN	Rucker	SIPR	76Q5/7182	ATO	12/20/2009
DA188863		SAM HOUSTON	SIPR	7966,754E,7PY3,7Q7F		
DA186758		SILL	SIPR	7QY5,7MJ6,7T05,7A83		
DA186788	LAN FT STEWART SIPR	Stewart/Hunter AAF	SIPR	75P1	IATO	9/15/2009
DA184429	7thSigCtr SIPRNet ITS	S-TNOSC	SIPR	7730 / 70M6	ATO	11/25/2011
DA768925		Watervliet Arsenal	SIPR	71ZF		
DA183184		West Point	SIPR	77M6		
		Yuma	SIPR	73XB	ATO	11/28/2009
-	7thSigCtr VTC	S-TNOSC	VTC		ATO	2/7/2010
		Detrick		233Z		9/7/2009
			_			

Entry Not official yet - in process of transfer

This page intentionally left blank.

Att 2-6
FOR OFFICIAL USE ONLY

ATTACHMENT 3. MEMORANDUM, USAF JUDGE ADVOCATE, SUBJECT: MEDICAL USE OF ENCRYPTED PHONE SYSTEMS AND SIPRNET, 14 APRIL 2004

The USAF Judge Advocate Memorandum follows.

Att 3-1 FOR OFFICIAL USE ONLY



DEPARTMENT OF THE AIR FORCE HEADQUARTERS UNITED STATES AIR FORCE WASHINGTON, DC

14 APR 2004

MEMORANDUM FOR HQ AFCA/JA

FROM: HQ USAF/JA 1420 AF Pentagon Washington D.C. 20330-1420

SUBJECT: Medical Use of Encrypted Phone Systems and SIPRNET

References: (a) Request for Legal Review of Medical Use of Encrypted Phone Systems and SIPRNET, 30 Sep 03

- (b) Permissibility of Encrypting Protected Medical Information in Communications to and from Fixed Medical Treatment Facilities under the Law of Anned Conflict, DoD/GC (Health Affairs), 28 Mar 03
- (c) Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field (12 August 1949) (GWS)
- (d) Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked of Armed Forces at Sea (12 August 1949) (GWS Sea)

Reference (a) requests a legal review of the use of SIPRNET and encrypted phone systems by medical facilities. This legal review discusses those provisions of the Law of Armed Conflict (LOAC) that affect secure electronic communications to and from modical facilities. We conclude that the installation and use of SIPRNET terminals and encrypted phone systems in modical facilities is permitted by LOAC, but only if the equipment is used for the exclusive purpose of medical operations.¹

Medical units and establishments organized for medical purposes, whether fixed, mobile, permanent or temporary, are protected from attack if they are exclusively engaged in the search for, collection, transportation, diagnosis or treatment, including first-aid treatment, of the wounded, sick and shipwrecked, or the prevention of disease. Medical facilities include hospitals, blood transfirsion centers, preventive medical centers and institutes, medical depots, and medical and pharmaceutical stores of such units.²

FOR OFFICIAL USE ONLY

Medical operations are limited to these actions reasonably necessary for the medical famility in perform its mission, which under LOAC is the securib for, collection, transportation, diagonary and treatment of womerled, sick and shipwrocled persons, and the prevention of disease.
 Article 19, GWS.

If a medical facility is used for acts inconsistent with its medical mission and protected status, or otherwise engages in acts harmful to the enemy, it may lose its protected status. Loss of its protected status can occur only after due warning has been made and the warning has been disregarded.³ The fact that a medical facility is protected by pickets, sentries, or armed escorts does not deprive it of the protection guaranteed by the Geneva Conventions."

Article 34 of GWS (Sea) provides that "hospital ships may not possess or use a secret code for their wireless or other means of communication." However, there is no corresponding prohibition that applies to land-based medical facilities. Therefore, the obligation of the U.S. armed forces is to maintain medical facilities for the excusive purposes of providing health care and to avoid using those facilities for any acts harmful to the enemy. Based on the forceoing, DoD/GC determined LOAC does not prohibit encrypted Internet/NIPRNET transmission of medical information to or from land-based medical facilities.⁵

DoD/GC also noted that in order to make it clear to encury forces that a medical facility is transmitting only medical information (and not intelligence information), there may be policy reasons to set up communications so that they flow unencrypted in a manner that would allow the medical facility to demonstrate its transmissions contain only modical information.⁶ Other alternatives would be to make provisions for a neutral third party to verify that a medical facility's transmissions contain only medical information, or to use systems that could be easily disconnected if necessary. However, these are policy considerations not legally required by LOAC.

The use of SIPRNET⁷ and encrypted phone communications⁸ by medical facilities relies on the same international law analysis as the use of encrypted Internet/NIPRNET systems. Consequently, we conclude that LOAC does not bar a medical facility from installing a SIPRNET terminal or an encrypted phone system to transmit or receive encrypted information, so long as the systems are used only for medical purposes. The presence of SIPRNET and encrypted phone systems in a medical facility does, however, create some unique policy considerations.

Because the SIPRNET was initially intended as a command and control tool, adversaries may be skeptical of U.S. claims that its modical facilities with SIPRNET terminals are using the

Z

⁹ Article 21, GWS.

Article 22, GWS.

⁵ See Permissibility of Energying Protected Medical Information in Communications to and from Fixed Medical Treatment Partletter under the Law of Armed Conflict, OSD/GC (Health Affairs). 28 Mar 03. This opinion supersedes earlier opinions by AF/JAO and other AF offices regarding the use of encrypted communications by incideal facilities.

⁴ This may, of course, subject the data to interception by a helligerent stohisticated enough to satisfy itself that the transmissions

The SIRNET has natured to be the core of our warlighting countered and control capability. Subset here within the DoD and other Government Agencies are able to use the SIPRNET for passing data at the Secret-Not Robusable to Foreign Nationals classification level. Although the SIPRNET was originally designed as a countered and control system, it is fast becoming the defects associated of preferred data services, even over the NPRNET * Encrypted phone equipment used by DoD typically consists of other the Secure Tokyhone Lhit - Third Generation (STU-III)

or he never digital-based Secure Terranal be upment (STE). The STU-IL is a low-cost, use "friendly, scoure telephone dework. The terrainals me designed to operate reliably, with high voice quality, as both ordinary selephones and secure instruments over the disi-up public switch telephone network. The Secure Terminal Equipment is the evolutionary successor to the STU-III. The STE program improves communications by changing our the spinlog STU-DI products with digital-based STE products.

terminals only for medical purposes. Therefore, for policy reasons commanders should consider some of the same safeguards suggested with respect to general energyted communications, such as making provisions for a neutral third party to verify that the system is being used only for medical purposes, or using systems that can be easily disconnected if necessary. It may also be useful to request State Department assistance in communicating to opposing beligerent governments the legitimate purposes of having secure communications in medical facilities.⁹ Commanders should also consider the practical security issues associated with placing classified equipment and information in medical facilities, such as the necessity for a secure repository and a secure area with limited access. Medical facilities that are in areas where they risk being captured will have to take reasonable measures, within the bounds of LOAC, to protect the encryption equipment and classified information.¹⁰

Use of encrypted phone systems and SIPRNET by medical facilities does not violate LOAC as long as information transiting the system is in furtherance of the medical mission. As with encrypted Internet/NIPRNET transmission of medical information, there are likely many ways in which the risks associated with using SIPRNET and encrypted phone equipment in medical facilities can be addressed, mitigated, and balanced against the potential benefits. We defer on such policy considerations, and leave it to MAJCOM Communications and Information Directorates to appropriately consider these issues when deciding whether the installation of specific encrypted equipment in a particular medical facility is appropriate. We do recommend that a thorough legal and policy review be conducted in each case before a system is installed. Reviewing authorities may want to require medical facilities to submit a detailed justification that includes information such as why the system is required, why removable equipment will not suffice, the particular medical uses for which the system will be used, a description of the type of medical information that will be encrypted, and the steps that will be taken to ensure the equipment will be used only for medical purposes. It may also be useful for general guidelines to be published by the appropriate agencies regarding these issues.

THOMAS J/FISCUS Major General, USAF The Judge Advocate General

ce: MAJCOM/IAs AFJAGS SAF/GC HQ AF/SG

⁹ For example, many aspects of military medical operations, such as casualty reporting, readiness status reports, and the protection of cortain patient information under U.S. are may require modical idealities to use secure communication channels. ¹⁰ The more presence of encryption equipment in a medical facility exacts social calculates to use secure communication channels, associates the the equiption, is being used safely for medical purposes. Likewise, if medical personnel destroy or disable the equipment in form falling into energy hands, the energy much question whether such actions fall within the medical personnel's burstnitarian daties – puring their protected status at risk. However, LOAC is ambiguous on this issue. There is no clear legal authority for medical purposes from being converted to broader military methods to LOAC to prevent equiption used solvely for medical purposes from being converted to broader military intelligence uses when capt ned by madiversery.

ATTACHMENT 4. E-MAIL, GSA, MR. POLLOCK, SUBJECT: QPL FOR COMBINATION PADLOCKS AND E3 CLASS, 4 MAY 2010

The GSA e-mail follows.

Att 4-1 FOR OFFICIAL USE ONLY

Jones, Ralph CIV USA AMC

From:	christopher.pollock@gsa.gov
Sent:	Tuesday, May 04, 2010 1:09 PM
To:	Jones, Ralph CIV USA AMC
Cc:	william.talbot@gsa.gov; jeffery.schatz@gsa.gov
Subject:	Re: Fw: QPL for Combination Padlocks (UNCLASSIFIED) and e3 class

Mr. Jones,

First let me introduce myself, my name is Chris Pollock and I am the engineer at GSA responsible for Federal Specification FF-P-110.

FF-P-110J , with Amendment 1 is still valid. Copies are currently available from the DLA ASSIST database. GSA will take action to post it on our website.

There is no QPL for this specification. There are no requirements in the Federal Specification for a QPL. Going back as far as at least 1992 there has only been one product determined to meet the requirements of the specification. Federal Standardization guidelines do not allow us to create a QPL when there would be only one item listed.

The S&G 8077 padlock is the only product I know of tested and approved to FF-P-110J and amendment 1 since at least 1992.

If you have any questions, or want to discuss further, please don't hesitate to contact me.

Sincerely, Chris Pollock Electrical Engineer General Services Administration Phone: (703) 605-9256 FAX: (703) 605-9445

> William G. Talbot/3QSAAA/CO/ GSA/GOV

05/04/2010 11:40 AM то

сс

Subject Fw: QPL for Combination Padlocks (UNCLASSIFIED) and e3 class

Pollock/3QSAAA/CO/GSA/GOV@GSA

1

Christopher G.

Att 4-2

FOR OFFICIAL USE ONLY

Chris,

You probably already got this from Jeff.

I'm waiting for a call back on the e3 class.

William ----- Forwarded by William G. Talbot/3QSAAA/CO/GSA/GOV on 05/04/2010 11:39 AM -----

"Jones, Ralph CIV USA AMC"	То
<ralph.jones@us.a< td=""><td><jeffrey.schatz@gsa.gov>,</jeffrey.schatz@gsa.gov></td></ralph.jones@us.a<>	<jeffrey.schatz@gsa.gov>,</jeffrey.schatz@gsa.gov>
rmy.mil>	<william.talbot@gsa.gov></william.talbot@gsa.gov>
	cc
05/04/2010 09:16	
АМ	Subject
	QPL for Combination Padlocks (UNCLASSIFIED)

Classification: UNCLASSIFIED Caveats: NONE
In doing SIPRNET installations, we use a lot of the Sargent & Greenleaf 8077 changeable combination padlocks. They are touted as meeting Fed Spec FF-P-110J. Questions have arisen over the validity of the locks and specification. Leading me to two questions.
1 - Is Fed Spec FF-P-110J (with Amendment 1) still valid? I couldn't find it listed on your GSA web site.
2 - Is there a Qualified Products List for this Fed Spec? Again, I couldn't find it listed on your web site. If there is one, could I get a copy in PDF file format?
Thank you for your assistance. If you have any questions or concerns, please contact me.

Ralph Jones USAISEC-FDED, Ft Detrick, MD cell: (240) 446-2818

2

Att 4-3

FOR OFFICIAL USE ONLY

This page intentionally left blank.

Att 4-4 FOR OFFICIAL USE ONLY

ATTACHMENT 5. E-MAIL, NSA CISSP, MR. ZUNDEL, SUBJECT: CNSSP 10 AND CNSSI 4005, 27 MAY 2010

The NSA e-mail follows.

Att 5-1 FOR OFFICIAL USE ONLY

Jones, Ralph CIV USA AMC

From:	Zundel, Norman D [ndzunde@nsa.gov]
Sent:	Thursday, May 27, 2010 10:08 AM
To:	Jones, Ralph CIV USA AMC
Cc:	Mansfield, Paul B.
Subject:	RE: CNSSP 10 and CNSSI 4005 (UNCLASSIFIED)
Signed By:	ndzunde@nsa.gov

Ralph,

The latest version of CNSSI 4005 that I have on the unclassified (low) side is from last November. Since then it has been undergoing NSA internal scrutiny. It is just about to be signed off by NSA and sent to the CNSS for their coordination process. When it does, the Army will get a formal (updated) copy on the unclassified system.

I was going to attached the November version, but it doesn't even have the section you are looking for. The decision to incorporate NSTISSP 10 came later.

The section currently reads: QUOTE 61. Security containers used in INFOSEC applications must meet the following requirements:

 GSA-approved Class 5 Information Processing System (IPS) containers that have been drilled for signal, power and cooling:

 are required for storage and on-line closed-door operation of any combination of computer systems, servers, data communications equipment and data storage devices;

 May be used to store keyed, on-line COMSEC equipment that supports nets/circuits terminated in spaces that are not continuously manned by appropriately cleared persons; and

May not be used to store classified documents.

b. GSA-approved Class 5 or Class 6 security containers that have not been drilled for signal, power, and cooling are required for storage of classified COMSEC documents, and for off-line storage of classified data storage media (e.g. removable hard drives, laptops, floppy disks, CDs, DVDs, tapes and data cartridges).

Waivers regarding security containers may be granted by appropriate Service Authorities within the Government Departments/Agencies/Services. UNQUOTE

Please note that the requirements above are no different from those in the current CNSSP 10. Yes, Mr. Cornish tried to relax them, and I also tried to do so, but we were not able to gain consensus in order to get a new document signed. Thus, we reverted to the old words.

Norman

Norman Zundel, CISSP, SAIC Contractor I513, Dorsey Road, (301) 688-7212

Att 5-2

1

FOR OFFICIAL USE ONLY

CACMB, FANX 3, (410) 854-2291 ndzunde@nsa.gov or zundeln@saic.com

-----Original Message-----From: Jones, Ralph CIV USA AMC [mailto:ralph.jones@us.army.mil] Sent: Tuesday, May 25, 2010 5:12 PM To: Zundel, Norman D Subject: CNSSP 10 and CNSSI 4005 (UNCLASSIFIED)

Classification: UNCLASSIFIED Caveats: NONE

I understand that you are developing the CNSSI 4005 document which will replace CNSSP 10. I have a question concerning that, as we use IPS containers for our SIPRNET implementations all the time. I am also in the process of developing a SIPRNET Installation Criteria document to assist the Army communicators in their own SIPRNET installations.

In CNSSP 10, Section 1 Paragraphs 2b and 2c, it stipulates that off-line network equipment, such as classified laptops or hard drives, cannot be stored in the IPS container housing the active network equipment, such as the switches and encryption devices. In a 2 May 2008 email that I received from Mr. Anthony Cornish in the NSA Office of IA Policy, he stated that CNSSP 10 was being revised and the revision would allow that. Also that in the interim we could go with the revised statement.

My question is how will this be addressed in CNSSI 4005?

I'm also curious as to whether there will be any other changes that may affect our use of IPS containers in our SIPRNET installations. To that end, would it be possible to obtain a draft copy of CNSSI 4005 (in PDF or DOC format) that I could use (and reference) in the development of my SIPRNET document?

Ralph Jones USAISEC-FDED, Ft Detrick, MD cell: (240) 446-2818

Classification: UNCLASSIFIED Caveats: NONE

Att 5-3 FOR OFFICIAL USE ONLY

This page intentionally left blank.

ATTACHMENT 6. FIGURE 2, DOD CUSTOMER CONNECTION PROCESS, FROM THE DISA CONNECTION PROCESS GUIDE, MAY 2010



Att 6-1 FOR OFFICIAL USE ONLY

This page intentionally left blank.

Att 6-2 FOR OFFICIAL USE ONLY

ATTACHMENT 7. APPENDIX F, DVS, FROM THE DISA CONNECTION PROCESS GUIDE, MAY 2010

Appendix F from the DISA connection process guide follows.

Att 7-1 FOR OFFICIAL USE ONLY

APPENDIX F

DVS – CLASSIFIED AND UNCLASSIFIED

This appendix provides the necessary steps and information for a DISN Video Services (DVS) connection. It is intended to supplement the detailed information provided in <u>Section 3</u> of this guide with DVS specific information. Any deviations from those steps or additional requirements are identified in this appendix.

F.1 DVS Connection Process

To obtain DVS service, the customer/sponsor must have an existing commercial Integrated Services Digital Network (ISDN) service and/or order a DISN transmission path DSN, Commercial or FTS). Information on ordering each of these services is provided in the service's appendix to this guide. Once the transmission path is obtained and corresponding ATC/IATC is granted, the customer/sponsor can then proceed with ordering the DVS service.

F.2 Process Deviations and/or Additional Requirements

Until additional hub resources are available, DVS-G registrations within CONUS will be limited only to those prospective sites with urgent valid requirement. Unless urgent, no new site registrations are being accepted. When required, DVS can facilitate "new" critical and/or urgent requirements on a case-by-case basis. Please contact the DCCC - DVS with the specifics of your request.

DVS-G Registration Process



(*) Site will receive automated email informing them to proceed to next step in registration process

Figure 15 DVS-G Registration Process

Att 7-2 FOR OFFICIAL USE ONLY

Item		DoD Customer		Non-DoD Customer	
		Existing	New	Existing	
Obtain OSD approval for Non-DoD connection			V		
Register the connection	1	\checkmark	√**	√**	
Register in the DVS-WS database	V	1	\checkmark	V	
Complete the CAP Package (Classified: Up to and including SECRET	Ń	V	~	V	
Access Approval Document	Ń	1	\checkmark	Ń	
Authority to Operate	V	1	\checkmark	V	
Topology Diagram	Ń	~	\checkmark	V	
Copy of Transport (DSN) ATC	V	1	V	V	
DAA Appointment Letter (If DAA is not SES or GO)	Ń	1	V	V	
Complete the CAP Package (Unclassified Sites)	V	V	V	V	
Authority To Connect Request	V	1	\checkmark	V	
Copy of Transport (DSN) ATC	V	1	\checkmark	V	
Topology Diagram	Ń	Ń	\checkmark	Ń	
Designate Primary Facilitation	V	1	V	V	
Complete DD Form 2875	V	1	1	V	
Complete JITC Verification	· √	\checkmark	V	V	
Complete AT&T Validation	N I	\checkmark	Ń	Ń	

F.3 DVS Connection Process Checklist

Table 5 DVS Checklist

Step 1 Complete Initial Registration with Business Development (BD)

- BD answers all questions, acts as primary POC to the customer through the registration process and refers them to the DVS-WS website <u>http://www.disa.mil/disnvtc/become.htm</u> to complete all required documents
- Upon online registration, customer provides required information. BD will assist the customer in completing this process as necessary
- BD then reviews the completed Site Profile, assigns a site ID and "Submits pending site" via DVS-WS
- After the site ID is assigned, BD tracks the process using DVS-WS "New Site Registration Queue"

Step 2 Submit CAP Documents to Communications Security (COMSEC) Manager

- Classified (up to and including SECRET) Sites: Customer completes an ATO and an Access Approval Document (AAD) (with DAA signatures) and submits them with a suite configuration drawing and a copy of the transport (DSN) ATC to the DVS COMSEC Manager for approval. Classified customers should allow 2-4 weeks to receive the COMSEC Keymat from the National Security Agency (NSA). Contact the CAD to register new transports (see POC information in <u>F.4</u>).
- Unclassified Sites: Customer completes ATC request with DAA signature (or the signature of a DAA designee) and submits it with a configuration drawing and a copy of the transport (i.e., DSN) ATC to the DVS COMSEC Manager. Contact the CAD to register new transports.
- COMSEC Manager reviews/approves all documents NOTE: If connection is Classified, COMSEC Manager orders KEYMAT for and checks the "Crypto approved" column in DVS-WS Site Registration Queue.

Step 3 Business Development Will Review Site Information

- · Reviews Site Profile information for any changes made since initial registration
- After the review is completed, BD checks "BD Approved" column in the DVS-WS New Site Registration Queue

Step 4 Designate Primary Facilitator with the Video Operations Center (VOC)

- Customer completes and submits a signed DD Form 2875 to the VOC designating a Primary Facilitator for the site (see POC information in <u>F.4</u>)
- VOC processes DD Form 2875 and checks the "PFAssigned" column in DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated e-mail is subsequently sent to the customers advising them to contact JITC to schedule Verification Test.

Step 5 Complete JITC Site Profile and Equipment/Facility Verification

- JITC verifies customer's site profile information and tests their equipment capabilities and room functionality. Classified customers must have already received an Over The Air Rekey (OTAR) from the VOC before performing the verification test
- Upon successful completion, JITC checks the "JITC Approved" column in the DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated e-mail is subsequently sent to customers advising them to contact AT&T to schedule a Validation Test.

FOR OFFICIAL USE ONLY

Step 6 Complete AT&T Validation

- · AT&T validates customers can connect to DVS-G as indicated on their site profile
- Upon successful completion, AT&T checks "AT&T Approved" column in the DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated e-mail is subsequently sent to customers advising them that the process is completed and that they can now schedule VTCs on DVS-G.

F.4 Points of Contact

DVS Connection Process POCs CONUS (Continental United States), DISA NS5			
Unclassified e-mail	dccc_dvs@csd.disa.mil		
Phone (Commercial)	800-554-DISN (3476)		
Phone (DSN)	312-854-4790		
Fax (Commercial)	703-681-3826		
Fax (DSN)	312-761-3826		

DVS Connection Process POCs Europe, DISA EU52			
Unclassified e-mail	vtcopseur@disa.mil		
Phone (Commercial)	011-49-711-68639-5260/5840/5445		
Phone (DSN)	314-434-5260/5840/5445		
Fax (Commercial)	011-49-711-68639-5312		
Fax (DSN)	314-434-5312		

DVS Connection Process POCs Pacific, DISA PC54			
Unclassified e-mail	vtcopspac@disa.mil		
Phone (Commercial)	808-656-0585		
Phone (DSN)	315-456-0585		
Fax (Commercial)	808-656-3838		
Fax (DSN)	315-456-3838		

DVS Connection Process POCs Southwest Asia (SWA), DISA NS5		
Unclassified e-mail	<u>vtcops@disa.mil</u>	
Phone (Commercial)	703-681-4111	
Phone (DSN)	312-761-4111	
Fax (Commercial)	703-681-3826	
Fax (DSN)	312-761-3826	

DVS Connection Process POCs DVS COMSEC Manager		
Unclassified e-mail	DVSTierIII@disa.mil	
Phone (Commercial)	703-681-4108	
Phone (DSN)	312-761-4108	
Fax (Commercial)	703-761-3826	
Fax (DSN)	703-681-3826	

FSO POC for Circuit and CNDSP Inquiries		
Contact Name	Robert Mawhinney, Chief	
	CNDSP & Planning Branch	
Unclassified e-mail	robert, mawhinney @ disa, mil	
Phone (Commercial)	717-267-9715	
Phone (DSN)	312-570-9715	

Designate Primary Facilitator with the VOC	
Unclassified e-mail	<u>VOC@disa.mil</u>
Phone (Commercial)	618-220-8688
Phone (DSN)	312-770-8688

AT&T Validation Test	
Phone (Commercial)	800-367-8722
Phone (DSN)	312-533-3000

JITC Certification Test	
Phone (DSN)	312-821-9333

DISN Customer Contact Center (DCCC)		
Unclassified e-mail	DCCC_DVS@csd,disa,mil	
Phone (Commercial)	800-554-DISN (3476), 614-692-4790	
Phone (DSN)	312-850-4790	

F.5 Additional Policy and Guidance Documents

DVS website: http://disa.dtic.mil/disnvtc/become.htm

F.6 Sample Topology Diagrams

All configuration drawings must include the make and model of the CODEC, IMUX, Dial Isolator, and all switches. This information is required prior to processing your request for service or renewal of service.

The Video Teleconferencing Facility (VTF) connectivity diagram must include all associated devices including video equipment, MCUs, line interface units, hubs, IP connections, routers,

Att 7-6 FOR OFFICIAL USE ONLY

firewalls, gateways, modems, encryption devices, backup devices, type of transport, bandwidth being utilized, your Site ID, and building/room locations of all equipment.



Figure 16 DVS Secure Configuration Drawing Example 1



Figure 17 DVS CAP Secure Configuration Drawing - Example 2





Figure 18 DVS CAP Secure Configuration Drawing – Example 3



Figure 19 DVS CAP Secure Configuration Drawing - Example 4





Figure 20 DVS CAP Secure Configuration Drawing – Example 5



Figure 21 DVS CAP Secure Configuration Drawing - Example 6



This page intentionally left blank.

Att 7-10 FOR OFFICIAL USE ONLY

ATTACHMENT 8. APPENDIX J, SIPRNET, FROM DISN CONNECTION PROCESS GUIDE, 22 JUNE 2009

Appendix J from the DISA connection process guide follows.

Att 8-1 FOR OFFICIAL USE ONLY

APPENDIX J

SIPRNET – CLASSIFIED

This appendix provides the necessary steps and information for a Secret Internet Protocol Router Network (SIPRNet) connection. It is intended to supplement the detailed information provided in <u>Section 3</u> of this guide with SIPRNet specific information. Any deviations from those or additional requirements are identified in this appendix.

J.1 SIPRNet Connection Process

Follow steps 1-12 in Section 3 of this guide.

J.2 Process Deviations and/or Additional Requirements

Step 8 DoD Contractor connections to the SIPRNet must go through the Defense Security Service (DSS) for accreditation of their facilities and information systems. For questions regarding DSS accreditation, contact the DSS SIPRNet Program Management Office at <u>disn@dss.mil</u> by phone at 888-282-7682, Option 2.

Step 10 All DoD and Non-DoD customers/sponsors must complete the SIPRNet Customer Questionnaire (SCQ) and submit it with the CAP package. The DAA is responsible for the content of the SCQ but may delegate the signatory responsibility to a lower level. The SCQ is available on the CCAO web page at www.disa.mil/connect/library.

- All 'Yes' responses must be explained
- All POC information must be completed for the questionnaire to be accepted by the CCAO

Step 11 The CCAO review of the SIPRNet CAP Package for new connections includes an online remote compliance assessment. This is a vulnerability scan of the IS requesting SIPRNet connection, performed by the CCAO, to identify possible vulnerabilities that exist within the IS. The results are used during the connection approval decision-making process.

J.3 SIPRNet Connection Process Checklist

This checklist provides the key activities that must be performed by the customer/sponsor during the SIPRNet connection approval process.

Item	DoD Customer		Non-DoD Customer	
nem	New	Existing	New	Existing
Obtain OSD approval for Non-DoD connection			1	√*
Provision the connection	1		1	√*
Perform the C&A process	V	\checkmark	N	V
Obtain an accreditation decision (ATO/IATO)	1	√	N I	V
Register the connection	1	√**	Ń	√*
Register in the GIAP/SGS database	V	√**	Ń	√*
Register in the PPSM database	V	√**	1	√*
Register in the SIPRNet IT Registry database	V	√**	1	√*
Register with Network Information Center (NIC)				
Complete the CAP Package	1	√	1	V
DIACAP Executive Package (or equivalent for Non- DoD entities)	\checkmark	V	Å	V
DIACAP Scorecard	V	√	Ń	V
System Identification Profile	V	\checkmark	Ń	1
Plan of Actions and Milestones, if applicable	V	V	Ń	V
DAA Appointment Letter	\checkmark	\checkmark	\checkmark	
Network/Enclave Topology Diagram	V	V	Ń	V
Consent to Monitor	1	1	Ń	V
SIPRNet Customer Questionnaire (SCQ)	V	√	Ń	V
Proof of Contract			Ń	V
OASD(NII) Approval Letter			Ń	√*
Submit the CAP Package to the CCAO	V	V	Ń	V
Receive remote compliance scan	\checkmark		N	
Receive SIPRNet ATC/IATC	V	V	1	V

Table 7 SIPRNet Connection Process Checklist

*This step is not required for existing Non-DoD Customer connections unless there has been a change in Sponsor, mission requirement, contract or location.

**This step is not required for existing connections that are already registered and all information is current.

J.4 Points of Contact

Network Information Center (NIC)	
Phone (Commercial)	800-365-3642
Phone (DSN)	312-850-2708
Fax (Commercial)	614-692-3452
Fax (DSN)	312-850-3452
Website	www.nic.mil

SIPRNet Service Manager	
Phone (Commercial)	703-882-2770

SIPRNet Support Center (SSC)		
Phone (Commercial)	800-582-2567/703-821-6260	

Classified Connection Approval Office (CCAO)		
Unclassified e-mail	CCAO@disa.mil	
Classified e-mail	CCAO@disa.smil.mil	
Phone (Commercial)	703-882-1455	
Phone (DSN)	312-381-1455	
Fax (Commercial)	703-882-2813	
Fax (DSN)	312-381-2813	

J.5 Additional Policy and Guidance Documents

Cross Domain Solutions (CDS) are a special case of the SIPRNet connection process. Please refer to the CDS Process (Appendix K) for more information.

J.6 Sample NIPRNET/SIPRNET Topology

All topologies must include:

- Topology date
- CCSD (preferably near premise router)
- IP addresses for all devices within the enclave, and the following devices must include additional information specific to them:
 - Firewalls: manufacturer, model, and software/firmware version
 - IDS: manufacturer, model, and software/firmware version
 - Servers: server function (i.e., OWA, Web Server, etc.) and operating system (including
 most updated Service Pack installed on system)
 - Workstations: operating system (including most updated Service Pack installed on system)



Note: Please relevance NAP at http://www.nim-cours.org/co-actionativati/ for compliant deute-listing

Figure 24 NIPRNET/SIPRNET Topology Sample 2



This page intentionally left blank.

Att 8-6 FOR OFFICIAL USE ONLY
ATTACHMENT 9. WHITE PAPER, NOVA DATACOM, DEPARTMENT OF DEFENSE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP), 2009

The Nova Datacom White Paper follows.

Att 9-1 FOR OFFICIAL USE ONLY

SIPRNET Technical Implementation Criteria October 2010



DEPARTMENT OF DEFENSE CERTIFICATION AND ACCREDITATION (DIACAP) PROCESS

A NOVA DATACOM WHITEPAPER

INTRODUCTION

All Department of Defense (DoD) information systems (IS) MUST be certified and accredited per the guidance in Department of Defense Instruction (DoDI) 8510.01, dated November 28, 2007.

The process described in this instruction is the Department of Defense Certification and Accreditation Process (DIACAP).

The DIACAP is a complex and lengthy process that is completed in five phases. This process can take months, or even years, depending on the size of the IS, the competence of the DIACAP team, and the availability and competence of the personnel responsible for completing the different aspects of the DIACAP process.

However, just because your IS is accredited does not mean that you can connect to the DoD. Once your IS is accredited, you must then request an Authority to Connect (ATC) before you can connect to the DoD.

The DIACAP defines the following activities for the certification and accreditation of a specific DoD Information System. These activities may occur concurrently or sequentially, or at varied frequencies for different Information Assurance (IA) controls. The DIACAP parallels the system life cycle, and its activities should be initiated at inception. However, failure to initiate the DIACAP at system inception is not a justification for ignoring or non - complying with the DIACAP. Regardless of the system life cycle stage, unaccredited systems shall initiate the DIACAP immediately. The implementation of IA and services will be less expensive and problematic if the DIACAP is initiated early in the system life cycle.

The entire DIACAP process is described below. The five phases of the DIACAP will be discussed followed by a discussion describing the process for obtaining the ATC.

Note: As of 1 July 2009, no further Department of Defense Information Technology Certification and Accreditation Program (DITSCAP) documents will be accepted.

PHASE 1:

INTIATE AND PLAN INFORMATION ASSURANCE (IA) CERTIFICATION AND ACCREDITATION (C&A)

This activity includes registering the system with the governing Department of Defense (DoD) Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIACAP Implementation Plan (DIP).

Register the System with the DoD IA Program.

System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. DIACAP registration facilitates organizational Information Technology (IT) management and Federal Information Security Management Act of 2002 (FISMA) reporting. It involves recording descriptive system acquisition and information assurance data in a manner as to allow unique system identification. Registration commences a dialog between the DoD information system owner and the DoD Component Chief Information Officer (CIO), which should continue until the DoD information system is decommissioned.

The set of information gathered during system registration is referred to as the System Identification Profile (SIP), which becomes part of the DIACAP package for the information system, and is

DIACAP Process Whitepaper

1

Att 9-2 FOR OFFICIAL USE ONLY

"All Department of Defense (DoD) information systems (IS) MUST be certified and accredited per the guidance in Department of Defense Instruction (DoDI) 8510.01, dated November 28, 2007."



maintained throughout the system's life cycle. The SIP identifies the minimum data requirements, plus explanations, for registering an information system with the Component. Typically, this information can be found in program/project documentation, such as the initial capabilities document, system requirements/specifications, architecture and design documents, etc.

Assign IA Controls

Identifying the baseline DoD Enterprise IA controls that apply to a particular IS is a critical DIACAP implementation activity. To execute this activity, an appropriate MAC and CL must be established for each IS. DoD Instruction 8500.2, "Information Assurance Implementation," identifies IA control sets applicable to a system specific MAC and CL designation. A DoD Component CIO, Mission Area (MA) Designated Approval Authority (DAA), local system DAA or official DoD Community of Interest (COI) representative may add additional IA controls, to locally augment the security stringency of baseline control set, only when the augmented controls increase the security stringency established by the enterprise baseline IA controls.

The baseline IA control sets are taken from DoDI 8500 - 2 IA Control Checklists. There are approximately 240 baseline IA controls that are taken from DoDI 8500 - 2. Further, there are additional augmented controls that are taken from the various regulations such as Army Regulation 25 - 2 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS). Generally speaking, there are hundreds of IA controls associated with the DIACAP process for an IS.

Assemble the DIACAP Team

The members of the DIACAP Team are required to meet the trustworthiness investigative levels for users with IA management access to DoD unclassified ISs. Senior Information Assurance Officers (SIAOs) shall meet the same investigative requirements as those for DAAs, and certification cadre members shall meet the same requirements as those established for monitoring and testing.

The DIACAP team members and their respective roles are identified below:

Designated Approval Authority (DAA) – The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority. The DAA is designated by the Principal Accrediting Authority (PAA) or the Heads of DoD Components, and is responsible for authorizing or denying the operation (or the testing) of the assigned DoD IS by issuing an accreditation decision. The possible accrediting decisions are: 1) Authority To Operate (ATO), 2) Interim Authority To Operate (IATO), 3) Interim Authority To Test (IATT), and 4) Denial of Authority To Operate (DATO). A DAA bases this decision on a recommendation of the Certifying Authority (CA), accompanied by supporting material from the DIACAP Comprehensive Package. A DAA may downgrade or revoke an accreditation decision any time risk conditions or concerns so warrant.

In addition to the responsibilities established in DoDI 8500.2, a DAAs is also expected to:

- Comply with Defense Information Systems Network (DISN)//Global Information Grid (GIG) Flag Panel direction issued on behalf of the GIG MA PAAs.
- Ensure a DIACAP package is initiated and completed for assigned ISs.
- Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.
- Ensure security classification guides are established according to DoD 5200.1 R.
- Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.

Senior Information Assurance Officer (SIAQ) – The Senior Information Assurance Officer is the official responsible for directing an organization's IA program on behalf of the organization's CIO. SIAOs are appointed by Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD CIO to direct and coordinate the DoD IA Program.

The SIAO has the following responsibilities:

- Establish and enforce the C&A process within the DoD Component IA program.
- Ensure DoD Component level participation in the DIACAP Technical Advisory Group (TAG).

2 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-3 FOR OFFICIAL USE ONLY

"'Information Assurance Implementation,' identifies IA control sets applicable to a system specific MAC and CL designation."





- Track the C&A status of ISs that are governed by the DoD Component IA program.
- Establish and manage a coordinated IA certification process for ISs governed by the DoD Component IA program. This includes functioning as the CA or formally delegating CA for governed ISs.
- Identifying and recommending changes and improvements to certification and validation procedures to the TAG for inclusion in the DIACAP Knowledge Service (KS).
- Ensuring that DoD Component certification guidance is posted to the DoD Component portion of the KS.
- Serve as the single IA coordination point for joint or Defense wide programs that are deploying ISs to DoD Component enclaves.
- Comply with DISN/GIG Flag Panel direction issued on behalf of the GIG MA PAAs.
- Ensure a DIACAP package is initiated and completed for assigned ISs.
- Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.
- Ensure security classification guides are established according to DoD 5200.1 R (Reference (n)).
- Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.

<u>Certification Authority (CA)</u> – The CA is the senior official having the authority and responsibility for the certification of all information systems governed by a DoD Component IA Program, and may designate a Certifying Agent to act on behalf of the Certifying Authority. The CA has the authority to formally evaluate the IA capabilities and services of a DoD Information system and issue a Certification Determination. This determination accompanies the DIACAP package for review by the DAA towards an accreditation decision. The CA continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts. The SIAO functions as the CA and formally appoints CA Representatives for all governed ISs.

<u>Program Manager (PM)/System Manager (SM)</u> – A Program or System Manager is the official responsible for and authority to accomplish program or system objectives for development, production and sustainment to meet the user's operational needs. Additionally, the PM serves as the focal point for the integration of IA into and throughout the system life cycle of an assigned DoD Information System.

The responsibilities of the PM/SM are:

- Ensure that each assigned DoD IS has a designated IA manager (IAM) with the support, authority, and resources to satisfy the responsibilities established in DoDI 8500.01.
- Implement the DIACAP for assigned DoD ISs.
- Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.
- Ensure that information system security engineering is employed to implement or modify the IA component of the system architecture in compliance with the IA component of the GIG Architecture and to make maximum use of enterprise IA capabilities and services.
- Enforce DAA accreditation decisions for hosted or interconnected DoD ISs.
- Develop, track, resolve, and maintain the DIACAP Implementation Plan (DIP) for assigned DoD ISs.
- Ensure IT Security Plan Of Action & Milestones (POA&M) development, tracking, and resolution.
- Ensure annual reviews of assigned ISs required by FISMA are conducted.

Information Assurance Manager (IAM).– The IAM is responsible for the overall information assurance program of a DoD information system or organization. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore IA posture.

Support the PM or SM in implementing the DIACAP.

3 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-4 FOR OFFICIAL USE ONLY



- Advise and inform the governing DoD Component IA program on DoD ISs Certification & Accreditation (C&A) status and issues.
- Comply with the governing DoD Component IA program information and process requirements.
- Provide direction to the IA Officer (IAO).
- Coordinate with the organization's Security Manager to ensure issues affecting the organization's overall security are addressed appropriately.

<u>User Representative</u> – The DoD Information System User Representative is the individual or organization that represents the user community for a particular system during the certification and accreditation process.

The User Representative is responsible for:

- Represent the operational interests of the user community in the DIACAP.
- Support the IA controls assignment and validation process to ensure user community needs are met.

Initiate the DIACAP Implementation Plan (DIP)

The DIACAP Implementation Plan contains both the strategy for implementation along with the current implementation status of assigned IA controls for a system. Specifically, this includes the Information System's assigned IA controls including inherited IA controls. The plan is part of the DIACAP package used by both the certifying authority and the designated accrediting authority for accreditation, and should be consistent with the program schedules.

The DIACAP Implementation Plan should contain the following, minimum information:

- Assigned IA controls -inherited and implemented
- Implementation Status
- Responsible entities
- Resources
- Estimated completion date for each IA control

Completing the DIP can be very time consuming – especially when trying to identify and contact the responsible entities. These are the people who are responsible for supervising, managing, or completing the various portions of the IA controls. Between vacations, business trips, meetings, etc., sometimes the DIP process can add significant additional time to the completion of the DIACAP.

PHASE 2:

IMPLEMENT AND VALIDATE ASSIGNED IA CONTROLS

This activity includes executing the DIP, conducting validation activities, preparing the IT Security POA&M, and compiling the validation results in the DIACAP Scorecard.

Execute the DIP

This activity includes all tasks related to the execution and resulting update of the DIACAP Implementation Plan, which describes the strategy and current status of the implementation of IA Controls for an information system. Each assigned IA Control is implemented according to the applicable implementation guidelines, which can be found in the description for an IA Control through the IA Controls section of the KS.

IA Controls may be individually validated as they are completed, or they may be validated by sub - entity of the DoD information system, Subject Area, or other organizing scheme established by the DIACAP Team. Therefore, implementation and validation activities may be occurring in parallel. The process of updating and maintaining a current reflection of the information system's IA posture should be continued throughout the system's life cycle. The DIP will continue to be updated as security relevant events impact the system's status.

4 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-5

FOR OFFICIAL USE ONLY





Conduct Validation Activities

Validation includes all tasks related to the execution of the validation procedures that are associated with assigned IA controls. For each IA control, one or more validation procedures have been developed which describe requisite preparatory steps and conditions, actual validation steps and expected results. Each procedure includes associated supporting background material, sample results, or links to automated testing tools. Validation procedures are maintained by the DIACAP TAG and published in the IA controls section of the DIACAP KS.

Actual results of the validation procedures are recorded according to the criteria and protocols specified in each procedure and are made a permanent part of the extended DIACAP package, along with any artifacts produced during the validation (e.g., output from automated test tools or screen shots that depict aspects of system configuration). For inherited IA controls, validation test results and supporting documentation are maintained by the originating IS and are made available to CAs of receiving ISs by request. Upon completion of the validation procedures, a POA&M is initiated to document non - compliance results and non applicable IA controls, if necessary. For any identified IA weakness, an associated Severity Category is assigned by the CA (and document-ed within the POA&M) to indicate the likelihood of the weakness being exploited.

The status of actual results for all assigned Validation Procedures is compiled into a DIACAP Scorecard. The status of assigned IA controls are indicated on the Scorecard as:

<u>Compliant (C)</u>. IA controls are those for which expected results for all associated validation procedures have been achieved.

Non - Compliant (NC). IA controls are those for which one or more expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk. Not Applicable (NA). IA controls are those that do not impact the security posture of the IS as determined by the DAA.

Prepare an IT Security POA&M

The purpose of an IT Security POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities. The Office of Management and Budget (OMB) requires agencies to prepare IT Security POA&Ms for all programs and systems where an IT security weakness has been found. The IT Security POA&M is designed to be a management tool to assist agencies in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. The DoD is responsible for maintaining the confidentiality of IT Security POA&M because they may contain pre - decisional budget information. The IT Security POA&M addresses: 1) why the system needs to operate, 2) any operational restrictions imposed to lessen the risk during the interim authorization, 3) specific corrective actions necessary to demonstrate that all assigned IA Controls have been implemented correctly and are effective, 4) the agreed upon timeline for completing and validating corrective actions, and 5) the resources necessary and available to properly complete the corrective actions. This section provides the instructions for filling out both the System level IT Security POA&M and the Component level IT Security POA&M.

IT Security POA&Ms are permanent records. Once posted, weaknesses will be updated, but not removed, after correction or mitigation actions are completed. Inherited weaknesses are reflected on the IT Security POA&Ms. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system - level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking the overall execution of system - level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system - level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA, the SIAO, and the governing DoD Component CIO. In order to reflect the complete IA posture of a DoD IS at all times in a single document, the IT Security POA&M is also used to docu-

5 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-6 FOR OFFICIAL USE ONLY



ment DAA - accepted NC IA controls and baseline IA controls that are NA because of the nature of the system.

DoD IT Security POA&Ms shall:

- Be tied to the agency's budget submission when required through the project identifier(s) of the system. This links the security costs with security performance. OMB Circular No. A - 11 requires that agencies develop and submit to OMB business cases for major IT investments. Additionally, each agency submits a list of both major and non - major IT investments. The agency assigns a project identifier(s) to each investment and includes it with these exhibits.
- Address all IT security weaknesses, including but not limited to those found during Government Account ability Office (GAO) audits, financial system audits, official security tests and evaluations or compliance reviews, and critical infrastructure vulnerability assessments.
- Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.
- Follow the format detailed below that is consistent with the examples provided by OMB.
- Be submitted to the DoD SIAO when directed.

DIACAP Scorecard

The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD Public Key Infrastructure (PKI) - certified digital signature. The DIACAP Scorecard contains a listing of all IA controls and their status of either C, NC, or NA.

Compliant (C) IA controls are those for which the expected results for all associated validation procedures have been achieved. Non - compliant (NC) IA controls are those for which one or more of the expected results for all associated validation procedures are not achieved. Not applicable (NA) IA controls are those that do not impact the IA posture of the IS as determined by the DAA.

All IA controls are labeled compliant, non - compliant, or not applicable. The results of IA control validation are annotated in the DIACAP scorecard. This scorecard, along with the associated POA&M, is evaluated by the DAA for an accreditation decision. The accreditation decision is annotated on the scorecard and becomes a part of the DIACAP package.

PHASE 3:

Make Certification Determination And Accreditation Decision

In this phase the Certification Authority (CA) makes the certification determination and the DAA makes the accreditation decision.

Make Certification Determination

When the system has completed all implementation and validation tasks, the DIACAP package is submitted to the Certifying Authority (CA) for a certification determination. A CA representative is an active member of the DIACAP Team from inception and continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts. Certification considers:

- The IA posture of the DoD information system itself. That is, the overall reliability and viability of the information system plus the acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself. The majority of this evidence comes from the implementation and validation evidence for the IA controls. Each control is validated according to the requisite validation procedures, and the expected results compared to the actual results give the CA an indication of the compliance status for each IA control.
- How does the system behave in the larger information environment? Does it introduce vulnerabilities to the environment? Does it correctly and securely interact with information environment management and control services? Is its visibility to situational awareness

6 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-7 FOR OFFICIAL USE ONLY

SIPRNET Technical Implementation Criteria October 2010





and network defense services adequate?

The Certification Determination is based on the actual validation results. It considers Impact Codes associated with IA controls in a non - compliant status, associated Severity Categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate. The weaknesses identified on the IT Security POA&M reflects residual risk to the system.

A certification determination is always required before an accreditation decision can be issued. If a compelling mission or business need requires the rapid introduction of a new DoD IS into the GIG, validation activity and a certification determination are still required. If the operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

As part of the certification decision, and after the individual IA controls have been validated as compliant, non - compliant, or not applicable, a residual risk analysis (an analysis that determines risk due to partial or unsatisfactory implementation of assigned IA controls) should be conducted. In order to determine the likelihood of a future adverse event, threats to a system must be analyzed in conjunction with potential vulnerabilities along with the IA controls that are in place for the system as well as the urgency of completing corrective action. Two indicator codes aid in this analysis: Impact Codes and Severity Categories.

Impact Codes are assigned to IA controls at the time of authoring and maintained by the DIACAP Technical Advisory Group (TAG). They indicate the TAG's assessment of the magnitude of network wide consequences of a failed IA control and are used to assess community risk. Impact codes are expressed as High, Medium, and Low, where High is the indicator of greatest impact or urgency. In conjunction with the severity category, it also indicates the urgency with which corrective action should be taken. Within a severity category, non - compliant IA controls should be prioritized for correction or remediation according to their impact codes.

Severity Categories are assigned to a system weakness or shortcoming by a CA or a designated representative as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as category (CAT) I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS in question. For instance, what may be a CAT I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves so that the overall risk to the system is reduced to a CAT II.

Make Accreditation Decision

An accreditation decision is issued by the DAA, and is communicated via the DIACAP Scorecard and accompanying IT Security POA&M, if required. Documentation (e.g., artifacts, actual validation results) supporting an accreditation decision will be provided in electronic form if requested by DAAs of interconnecting systems. The accreditation decision is expressed as an ATO, IATO, IATT, or DATO. Absent an accreditation decision, a system is considered unaccredited.

The accreditation decision always applies to a specifically identified DoD IS and is based on a balance of mission or business need, protection of personal privacy, protection of the information being processed, and protection of the information environment, and thus, by extension, protection of other missions or business functions reliant upon the shared information environment.

The formulation of an accreditation decision is supported by the DIACAP package, and always requires a certification determination. If the validation is abbreviated due to mission urgency, the accreditation decision cannot exceed an IATO. If operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

When there is compelling operational necessity, DoD ISs may be allowed to operate despite IT security weaknesses that cannot be corrected or adequately mitigated within prescribed timeframes because of technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented. The DoD IT Security POA&M is used to document DAA ac-

DIACAP Process Whitepaper

7

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-8 FOR OFFICIAL USE ONLY



cepted non - compliant IA controls and baseline IA controls that are not applicable.

Authority To Operate (ATO)

Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years. The conditions are as follows:

- The ATO accreditation decision must specify an Authorization Termination Date (ATD) that is within three years of the authorization date.
- A system with a CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. When requested by an affected military commander, the DoD Component CIO shall authorize operation of a system with a CAT I weakness through an IATO. This responsibility cannot be delegated below the DoD Component CIO, and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO and the system's DAA.
- A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.
- An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA."

Interim Authority To Operate (IATO)

An IATO is a temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.

An IATO accreditation decision is intended to manage IA security weaknesses while allowing system operation. It is not intended to be a device for signaling an evolutionary acquisition. A version of a DoD IS acquired in one of a planned series of acquisition increments or development spirals should be granted an ATO, even if additional or enhanced capabilities and services are planned for future increments or spirals. Conditions are as follows:

- The IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days.
- A request for an IATO must be accompanied by a DIACAP POA&M. Corrective actions specified in the IT Security POA&M must be achievable within the authorization period and must be resourced accordingly.
- If CAT II weaknesses have not been corrected or satisfactorily mitigated after system operation under IATOs for a total of 360 days, the DAA will normally issue a DATO that will remain in effect until all corrective actions identified in the IT Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO.
- The DoD Component CIO may authorize continuation of operation under an IATO for systems with CAT II weaknesses that have operated for 360 consecutive days. This responsibility cannot be delegated below the DoD Component CIO. The DAA must certify in writing or through DoD PKI-certified digital signature that continued system operation is critical to mission accomplishment. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.

Interim Authority To Test (IATT)

An IATT is a temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

Authorization is based on an assessment of impact to the information environment, or in the case

8 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-9

FOR OFFICIAL USE ONLY





of live data, an assessment of mission impact. In many cases, not all IA controls need to be satisfied for testing. In concert with the PM/SM, the DAA will determine what IA controls must be satisfied for a specific testing event. The IATT accreditation decision establishes the agreed upon test duration and any special conditions or constraints, to include notification thresholds and addressees. Conditions include:

- The IATT accreditation decision is a special case for authorizing testing in a live information environment or with live data for a specified time period. IATTs should be granted only when operational environment/live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical).
- All applicable IA controls should be tested and satisfied prior to testing in an operational environment or with live data except for those which can only be tested in an operational environment. In consultation with the PM or SM, the DAA will determine which IA controls can only be tested in an operational environment.
- An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate. Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).

Denial of Authority To Operate (DATO)

A DATO is a DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

A DATO will be issued if the DAA determines that a DoD IS should not operate because the IA design is inadequate, assigned IA controls are not adequately implemented, or because of a lack of other adequate security is revealed through certification activities and there are no compelling reasons to allow system operation.

PHASE 4:

MAINTAIN AUTHORIZATION TO OPERATE AND CONDUCT REVIEWS Maintain Situational Awareness

Continued authorization to operate is contingent upon the sustainment of an acceptable IA posture, which is accomplished through ensuring continued compliance with assigned IA controls, and by maintaining a current and appropriate Authorization Decision. The DoD IS IAM has primary responsibility for maintaining situation awareness and initiating actions to improve or restore IA posture.

Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM continuously monitors the system or information environment for security - relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations.

Security relevant events may include:

- Expiration of an IA control re -validation period -Certain IA controls will have assigned re -validation periods in which the IA control must be re - validated.
- Security events defined by the IA control -The IAM must also remain cognizant of the IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations, e.g., penetration testing.
- Significant changes to an information system -Configuration changes to the system or information environment could impact the IA posture of the system. In addition, the IAM may, independently or at the direction of the CA or DAA, schedule a revalidation of any or

9 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-10 FOR OFFICIAL USE ONLY



all IA controls at any time. FISMA requires revalidation of a select number of IA controls at least annually.

DoD ISs with a current ATO that are found to be operating in an unacceptable IA posture through GAO or IG audits, or other reviews or events, such as an annual security review or compliance validation, shall have the newly identified weakness added to an existing or newly created IT Security POA&M.

If a newly discovered CAT I weakness on a DoD information system operating with an ATO cannot be corrected within 30 days, the system can only continue operation as follows:

A system with a CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. When requested by an affected military commander, the DoD Component CIO shall authorize operation of a system with a CAT I weakness through an IATO. This responsibility cannot be delegated below the DoD Component CIO, and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO and the system's DAA.

If a newly discovered CAT II weakness on a DoD IS operating with a current ATO cannot be corrected or satisfactorily mitigated within 90 days, the system can only continue to operate as follows:

The DoD Component CIO may authorize continuation of operation under IATO for systems with CAT II weaknesses that have operated for 360 consecutive days. This responsibility cannot be delegated below the DoD Component CIO. The DAA must certify in writing or through DoD PKI certified digital signature that continued system operation is critical to mission accomplishment. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.

Maintain IA Posture

Sustainment of an adequate IA posture is accomplished through ensuring continued compliance with identified IA controls and by maintaining a current and appropriate Authorization Decision. The DoD information system IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore an acceptable IA posture.

The IAM may recommend changes or improvement to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements to the design of the information system itself.

Perform Reviews

The IAM shall annually provide a written or DoD PKI - certified digitally signed statement to the DAA and the CA that indicates the results of the security review of all IA controls and the testing of selected IA controls as required by FISMA. The review will either confirm the effectiveness of assigned IA controls and their implementation, or it will recommend changes to the accreditation status (e.g., accreditation status is downgraded to IATO or DATO); or development of an IT Security POA&M. The CA and DAA shall review the IAM statement in light of mission and information environment indicators and determine a course of action that will be provided to the concerned CIO or SIAO for reporting requirements described in FISMA. The date of the annual security review will be recorded in the SIP. A DAA may downgrade or revoke an accreditation decision at any time if risk conditions or concerns so warrant.

Initiate Reaccreditation

In accordance with OMB Circular A - 130, an IS must be recertified and reaccredited once every three (3) years. The results of an annual review or a major change in the IA posture at any time may also indicate the need for recertification and reaccreditation of the IS.

Att 9-11 FOR OFFICIAL USE ONLY





PHASE V: DECOMMISSION Decommission

When a DoD IS is removed from operation, a number of DIACAP - related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, Lines 8, "DIACAP Activity," and 9, "System Life Cycle Phase," of the SIP should be updated to reflect the IS decommissioned status. Concurrently, the DIACAP Scorecard and any POA&Ms should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management should be reviewed for impact.

The program manager should coordinate with DoD governing GIG activities, as appropriate, to identify and apply applicable decommissioning requirements necessary to eliminate the functional or military capabilities of systems. Decommissioning requirements and procedures change over time as the GIG enterprise information environment changes and are maintained through by the DIACAP TAG.

CONCLUSION

The DoD C&A and connection processes can be daunting. A system must first be certified and accredited via the five phase DIACAP process.

Once the DIACAP process has been completed, an IS then requires an IATC or ATC in order to connect to the network.

This process can be plagued with obstacles and roadblocks. It can take anywhere from 6 months to 2 years to complete the entire process.

For many people in DoD responsible for the DIACAP process it is an additional duty that interferes with their daily responsibilities. And because it may also be a new process to them, they have a lack of understanding of how the process works. Many DIACAP practitioners do not fully understand the process themselves. Further, the DIACAP process is constantly changing and adapting to new threats and technologies. Most think they can just "get by" when completing the DIACAP and then they do not have to worry about it for another 3 years. It would be great if it really worked that way.

Because of the way the DIACAP process is approached, with a sense of dread and foreboding, those in responsible positions, such as the Information Assurance Manager, just want to get it done and over with. This is one reason that DoD ISs are not as secured as they could be and adversaries are able to penetrate the systems.

We at Nova Datacom can provide a very important and needed service by helping those responsible to complete a high quality, efficient, and effective DIACAP process. Our goal should not be just "get it done", but actually build security into the system in order to successfully fight "Cyber Warfare".

11 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-12 FOR OFFICIAL USE ONLY



ABOUT THE AUTHOR

Timothy Taylor, CISSP, Information Assurance Engineer

Mr. Taylor recently retired from the U.S. Army with 31 years of honorable service. He has over 10 years of Information Security experience in addition to a combination of over 20 years Emergency Response, DoD Telecommunications, Physical Security, and Investigative experience. He has managed all activities related to the "Maintain Accreditation" phase of the Department of Defense Information Assurance Certification and Accreditation Program (DIACAP) for the U.S. Army Corps of Engineers Secure Internet Protocol Router Network (SIPRNet) and Managed computer security and information assurance support for the U.S. Army National Guard Headquarters. He has served as a Government Information Assurance Manager and an Active Agent of the Certification Authority (ACA) team member for National Guard Headquarters. He has coordinated and managed the National Guard's Information Technology Requirements Control Board (ITRCB).

Mr. Taylor holds a Masters Degree in Homeland Security, specializing in Security Management. He also holds a B.A. in Public and Criminal Justice Administration. Mr. Taylor has a Top Secret clearance with Sensitive Compartmented Information (SCI) eligibility. He is a Certified Information Systems Security Professional (CISSP) and a Certified Computer Examiner (CCE).

Relevant positions include:

- Nova Datacom / U.S. Army Corps of Engineers (USACE) Information Assurance Engineer
- U.S. Army National Guard Headquarters Tactical Communications Branch Telecommunications Operations Chief
 - Certification Authority Agent
 - Information Systems Technician
 - Systems Administrator/Global Command and Control Systems (GCCS) Analyst
 - Chief Information Officer (CIO), C6 Operations
 - Physical Security Manager
 - Continuity of Operations (COOP) Team Member
- U.S. Army / U.S. Army Criminal Investigation Command (CID) Special Agent
 - Counter Terrorist Team
 - White Collar Crime Team

12 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-13 FOR OFFICIAL USE ONLY





APPENDIX

AUTHORITY TO CONNECT (ATC) SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)

DISA is the connection approval authority for all DISN connections. The network that supports classified Internet Protocol (IP) based communications is the SECRET Internet Protocol Router Network (SIPRNET).

Under the authority of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, Defense Information System Network and Connected Systems, 9 July 2008, the DISN, Classified Connection Approval Office (CCAO) is responsible for monitoring the security compliance of SIPRNET customers. Its mission is to ensure that:

- Customer enclaves are compliant with established directives and guidance, and meet all technical and interoperability requirements.
- 2. Operational requirements have been met and validated.
- Customer sub networks, systems, and other connected components provide adequate security and have been accredited by the proper authority.
- 4. Customers meet established connection requirements.
- Customers are assessed through the use of remote compliance tools and they have met security standards.

The Classified Connection Approval Team assesses operational networks and enclaves with requirements for connection to the SIPRNet. The Team performs the necessary evaluation, analysis, review and assessment of customer enclaves including remote vulnerability scanning and validation. The CCAO ensures that all connections meet technical and interoperability requirements, sub - networks, subsystems and other connected components provide enclave accreditation documentation, and that security requirements have been implemented as required by DoD and DISA directives, instructions, and guidance. Additionally, the Team coordinates site compliance visits of SIPRNet customers with the DISA's Field Security Operations (FSO). The CCAO monitors the resolution of FSO's findings and the compliance of the customer's enclave/network connection to the SIPRNet.

Mandatory Requirements for an ATC for DOD Activities

- A complete Executive Package IAW DODI 8510.01, Enclosure 3, The DIACAP Package, dated 28 November 2007, must be submitted to the CCAO. SIPRNet customers will only be granted an ATC for a maximum of three years.
- SIPRNet Connection Questionnaire, dated 01 November 2008 (includes the Consent to Monitor).
- 3. Enclave Topology Diagram -Most recent configuration to include firewall(s), IDS, PC's, user terminals, servers, hubs, bridges, routers, major applications, gateways, modems, card readers, backup devices, room and building number, and switches (mechanical A/B or electrical), backside connections, Internet Protocol (IP) addresses, encryption devices and Cross Domain Solutions (CDS)/boundary crossing/interface devices). The topology must include the model number(s) and IP's of the devices on the diagram. The diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections). Other SIPRNet connections, (access points) must be shown. The flow of information to, from, and through all connections, Router Port SIPRNet (RTPS), host IP addresses, and CCSD number, if known must be shown. The topology must be dated and signed by the IAM/IAO.
- 4. Successful completion of a remote compliance assessment by the DISN, CCAO Team.
- All SIPRNet IP's must be registered.
- Indicate and label all of the devices, features, or information. Diagram minimum size: 8.5"x 11".

It is important to note that in accordance with DoD and DISA guidance, firewalls and Intru-

13 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-14 FOR OFFICIAL USE ONLY



sion Detection Systems (IDS) are required on all customer enclaves. Approval for connection to the SIPRNet will not be granted unless an approved firewall and IDS have been included in the customer's configuration and are compliant with published guidance. Private IP addresses (nonroutable) are not permitted on SIPRNet enclaves.

ATC FOR NON-SECURE INTERNET PROTOCOL ROUTER NETWORK (NIPRNET)

The rules are similar but less strict for the NIPRNet. However, the IS has to have an ATO or IATO and a network topology diagram before an Authority to Connect will be granted.

REFERENCES

- Army Regulation (AR) 25 2, 24 Oct. 2007, Information Management/Information Assurance
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, 9 Jul. 2008, DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY AND RESPONSIBILITIES
- 3. Defense Information Systems Agency (DISA), Knowledge Service
- Defense Information Systems Agency (DISA) Field Security Operations, Department of Defense Instruction (DoDI) 8500 - 2, 28 Mar 2008, IA Control Checklists
- Department of Defense Instruction (DoDI) 8500.01, 28 Nov. 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Department of Defense Instruction (DoDI), 8500.2, 6 Feb. 2003, Information Assurance (IA) Implementation

For additional information, please contact us at novasales@novadatacom.com to schedule a site visit and/or learn more about our IT contingency/disaster recovery and information assurance solutions.

14 DIACAP Process Whitepaper

Copyright (C) 2010 Nova Datacom LLC. All Rights Reserved

Att 9-15

FOR OFFICIAL USE ONLY

This page intentionally left blank.

Att 9-16 FOR OFFICIAL USE ONLY