SECURE WIRELESS LOCAL AREA NETWORK ADDENDUM to the WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

31 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
1.1 Background 1
1.2 Authority 1
1.3 Scope 1
1.4 STIG Distribution 2
1.5 Document Revisions 2

2. SWLAN COMPONENTS 3
2.1 SecNet 11 Components 3
2.1.1 SecNet 11 Plus PC Wireless NIC 3
2.1.2 SecNet 11 Wireless Bridge/Access Point 4
2.1.3 DTD 4

3. APPROVED SWLAN USE CASES 5

4. APPROVAL PROCESS FOR CONNECTING SECNET 11 TO THE SIPRNET 7
4.1 The Certification and Accreditation Process 7
4.2 SIPRNet Connection Approval 7
4.3 SWLAN Considerations 7
4.3.1 SWLAN Connection Approval 8
4.3.2 SWLAN Requirements 9

APPENDIX A. RELATED PUBLICATIONS 11

APPENDIX B. LIST OF ACRONYMS 13

TABLE OF FIGURES

Figure 3-1. LAN Extension..... 5
Figure 3-2. Wireless Bridging..... 6

LIST OF TABLES

Table 4-1. Connection Approval Steps for Wireless Connection to the SIPRNet..... 8
Table 4-2. SWLAN Requirements..... 9

1. INTRODUCTION

1.1 Background

This *Secure Wireless Local Area Network* (SWLAN) *Addendum to the Wireless Security Technical Implementation Guide* (STIG) is published as a tool to assist in the effective deployment of SWLANs within the Department of Defense (DOD). This Addendum is meant for use in conjunction with the *Wireless STIG*. The intent is for the information in this Addendum is to supplement and enhance the security requirements found in the *Wireless STIG*, by providing more specific and detailed configuration and management guidance on connecting and using secure wireless networks on the Secure Internet Protocol Routing Network (SIPRNet). This Addendum provides detailed guidance on the SIPRNet approval process as well as the currently approved SWLAN equipment and architectures.

Section 2, SWLAN Components, provides a technology primer describing the various components approved for use in the SWLAN. *Section 3, Approved SWLAN Use Cases*, details the two currently approved overarching use cases. *Section 4, Approval Process for Connecting SECNET 11 to the SIPRNet*, gives guidance on the approval process which must be followed when implementing a SWLAN and connecting the SWLAN to the SIPRNet and its enclaves.

Wireless architectures, devices and systems that are not specifically and approved by the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) are not authorized for connection to the SIPRNet. Unapproved wireless products may not be used to store, process, or transmit classified DOD information. The *Secure Wireless LAN CONOPS* discusses several architectures, which have been reviewed by the DSAWG. This document will be updated as additional architectures and products are approved by the DSAWG.

It should be noted that FSO support, for the STIGs, STIG Addendums, Checklists, and Tools, is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that “all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this Addendum will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing sensitive information.

1.3 Scope

This Addendum is designed to assist sites that are planning to connect to the SIPRNet using wireless products.

1.4 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG or Addendum, from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@ disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

2. SWLAN COMPONENTS

The National Security Agency (NSA) has certified the Harris Corporation's SecNet 11® Plus SWLAN product family for processing data classified up to and including Secret. This wireless product provides transparent, NSA-certified Type 1 encryption in a WLAN environment. When configured using an authorized architecture such as those discussed in *Section 3, Approved SWLAN Use Cases*, the SWLAN can provide mobility and rapid deployment to meet a wide range of command and control mission requirements.

Harris Corporation is developing a new NSA Type 1 certified WLAN product called the SecNet 54® which will provide a WLAN based on the IEEE 802.11a, b, or g standards (depending on which radio adapter is used). The SecNet 54 is expected to be available in third quarter 2005 and will be certified to process classified information up to Top Secret. Requirements for the SecNet 54 will be added to this Addendum when the card is approved for use.

NSA distributes both classified and unclassified operational keys for the SecNet 11 WLAN; therefore, SecNet 11 is available for unclassified WLANs that process highly sensitive information. Communications Security (COMSEC) or Department of Defense Activity Address Code (DODAAC) accounts are required for organizations that plan to use the SecNet 11, regardless of classification level.

The SecNet 11 product family includes: The SecNet 11 Plus PC card, the SecNet 11 Wireless Bridge, and the SecNet 11 Key Fill Cable. The following sections provide more detail on these components.

2.1 SecNet 11 Components

2.1.1 SecNet 11 Plus PC Wireless NIC

The SecNet 11 wireless network interface card (NIC) uses the Harris Sierra® Encryption Module, Intersil PRISM® II chipset, and Baton encryption algorithm. The card operates in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band using a modified Institute of Electrical and Electronics Engineers (IEEE) 802.11b protocol, which takes into account crypto delays. The cryptographic function is embedded in the card, making the card a controlled cryptographic item (CCI), even in an un-keyed state. SecNet 11 provides the capability to send and receive secure data, voice, and video between and among wireless stations in a cryptographically secure mode.

Unlike other wireless NICs, both the data and source/destination addresses are encrypted making it difficult to eavesdrop on the wireless transmission. The 802.11b frames are encrypted regardless of type (i.e., data, control, or management frames avoiding a number of the most popular wireless security exploits possible when using other commercial wireless products). Because of this added layer of encryption, SecNet 11 products cannot interoperate with any other commercial WLAN products.

The SecNet 11 Plus WLAN card is a Type II PCMCIA card. The card has an external, removable antenna. To enable the functionality of the SecNet 11 Plus PC card, the System Administrator (SA) must load the card driver and management utility onto the laptop or host computer. The card is inserted into the host computer's Type II PCMCIA slot. Next the SecNet 11 Key Fill Cable is used to connect the card to an N/CYZ-10 Data Terminal Device (DTD). Finally, the DTD is used to perform a key fill operation.

NSA's certification of the SecNet 11 Plus PC card does not include either the host computer's software or hardware. Also, the certification includes the software on the CD packaged with the SecNet 11 products. The host computer's software and hardware must be configured in accordance with all policies governing the connection of systems to the SIPRNet.

2.1.2 SecNet 11 Wireless Bridge/Access Point

The SecNet 11 Wireless Bridge provides wireless infrastructure support and wired network access for the SWLAN. Like most wireless bridges, this product may be configured for use as a wireless bridge (WB) or as an access point (AP). In the architectural drawings in *Section 3, Approved SWLAN Use Cases*, the devices are labeled as AP or WB to match the functionality for which the SecNet 11 Wireless Bridge is configured. A SecNet 11 Plus PC Card must be inserted into the SecNet 11 Wireless Bridge to provide wireless communications. Because the wireless bridge provides access to the SIPRNET, strict physical security and configuration controls must be used to protect the device at all times.

When configured as an AP, this product provides access for wireless clients to both the wireless and wired (SIPRNET) networks. When configured as a wireless bridge, this product can connect two independent networks into a single seamless network. Regardless of configuration, this device will only allow traffic from a client or bridge with a SecNet 11 Plus PC Card containing the appropriate (identical) key.

2.1.3 DTD

The key fill cable is used to transfer electronic encryption keys from the Key Fill Cable and Data Transfer Device (DTD) (AN/CYZ-10) to the SecNet 11 Plus PC card. Both are controlled items and must be strictly tracked by a COMSEC custodian.

3. APPROVED SWLAN USE CASES

The DSAWG has currently approved the NSA *Secure Wireless LAN CONOPS.* Organizations should leverage the architectures detailed in the CONOPS by tailoring them to meet their specific operational needs. For all architectures, wireless APs must be physically secure and an alarm or alerting method must be in place. For mission critical systems, an alternate communication method must be available in case of compromise. The CONOPS organizes the SWLAN implementations into two overarching use cases, which have been approved by the DISN Flag Panel. These overarching use cases are as follows:

LAN Extension: This architecture provides wireless access to the wired infrastructure using a Harris SecNet 11. In this architecture, the boundary is controlled either with fencing or inspection.

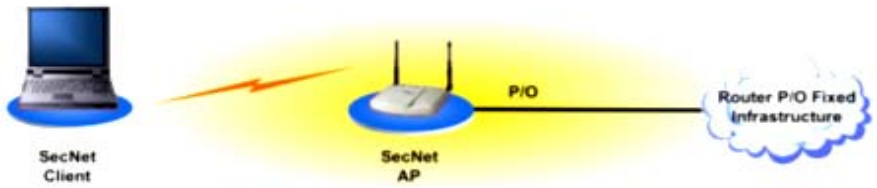

Figure 3-1. LAN Extension

Wireless Bridging: This architecture provides point-to-point bridging using Harris SecNet 11. In this architecture, the boundary is controlled either with fencing or inspection. All physical cable runs must comply with guidance specified in the *NAVSO P-5239-22: Protected Distribution System (PDS) Guidebook.*

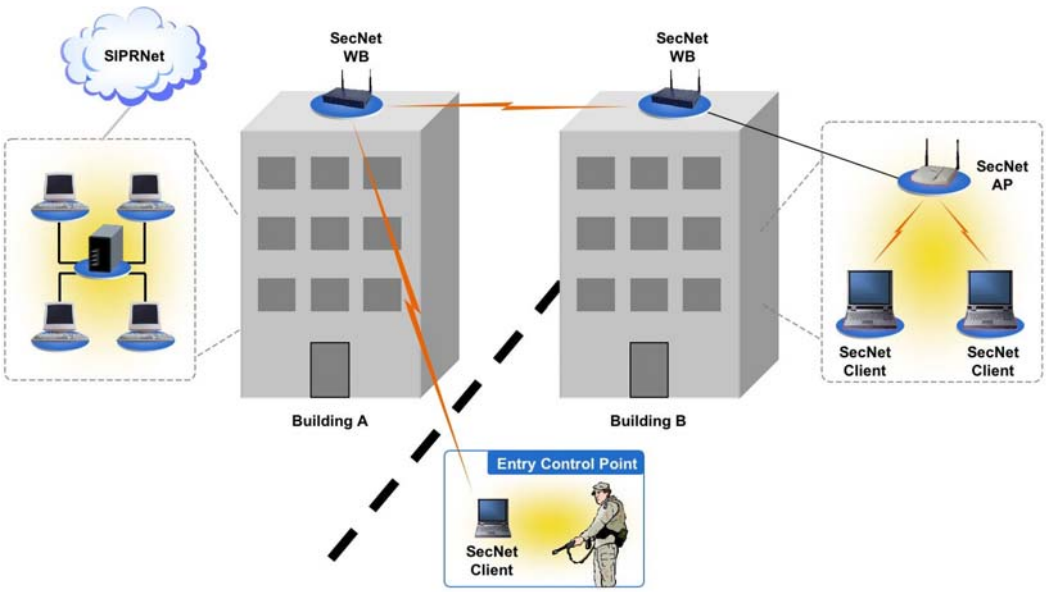

Figure 3-2. Wireless Bridging

At the time of the publishing of this document, proposed SWLAN architectures that fit specifically within the above overarching use cases can be approved without DSAWG review. Sites may modify existing use cases or propose new architectures or uses cases by following the process outlined in *Section 4, Approval Process For Connecting SecNet 11 to the SIPRNET*.

4. APPROVAL PROCESS FOR CONNECTING SECNET 11 TO THE SIPRNET

All systems must go through the Certification and Accreditation Process and obtain SIPRNet connection approval. The following sections describe the required steps for wireless network design, approval, and obtaining SIPRNet connection approval.

4.1 The Certification and Accreditation Process

All proposed SWLANs must be certified and accredited in accordance with DOD Instruction 5200.40, DITSCAP and DOD Manual 8510.1, DITSCAP Application. See *CJSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes,* for further information on policies, responsibilities and the connection approval process. Also refer to Appendix D of the *Secure Wireless LAN CONOPS* which provides a Certification & Accreditation and Connection Approval Process checklist that can be used to ensure all required DITSCAP and CAP steps have been followed.

4.2 SIPRNet Connection Approval

A Connection Approval Process (CAP) Package must be submitted to the SIPRNet Connection Approval Office (SCAO), who will approve all SWLANs before connection to the SIPRNet. In order to obtain direct wireless SIPRNet connectivity, the following main efforts must be completed:

- An initial modeling request
- A Request For Service (RFS)
- Security Accreditation documentation through the DITSCAP Process
- Individual Use Case approval by the DSAWG

A key component of a CAP package for wireless systems is written DAA approval. If the system is not accredited, the DAA must indicate if the system is operating under an Interim Approval to Operate (IATO). The SIPRNet connection will not be granted unless evidence of an accreditation or IATO is provided. If an IATO has been granted, the SCAO must be notified of all significant risks under which the system is currently operating. Such risks may include lack of identification and authentication mechanisms, lack of audit function, unprotected connections to other networks, and unauthenticated and unprotected dial-in capabilities. All connection requests must provide the following statement:

> "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on the connected host systems to determine the security features in place to protect against unauthorized access or attack."

4.3 SWLAN Considerations

This section provides additional guidance to facilitate the implementation of SWLANs.

4.3.1 SWLAN Connection Approval

Table 4.1, Connection Approval Steps for SWLAN Connection to the SIPRNet, provides a high level overview of the connection approval process. Part of the approval process includes determining if the intended functionality and architecture of the proposed SWLAN matches that of an approved use case. Organizations planning to install SWLANs should ensure that their proposed implementation complies with an approved uses cases. If the proposed implementation does not match an existing, approved use case, then the organization will work with NSA, the DSAWG and the DISA SCAO to get the security evaluation required for final approval and implementation.

One of the first steps in the SCAO review process for all SWLAN connection requests will be to determine if the system is consistent with the architecture of one of the approved use cases. If the site's selected SWLAN architecture is consistent with the architecture of any of the DSAWG approved use cases, the site is not required to present before the DSAWG unless specifically directed to do so by the SCAO. Such direction will be to resolve accreditation issues beyond the approval levels delegated to the SCAO, not merely for the presence of SWLAN technologies. Agencies planning to implement an approved SWLAN use case should contact the SCAO to discuss technical requirements for the specific use case selected before the CAP package is submitted. For non-approved SWLAN use cases or non-approved architectures of approved use cases, agencies seeking approval to connect to the SIPRNet must follow the same DITSCAP and SCAO submission process.

Connection Approval Steps	Required
Develop SWLAN system architecture.	X
Complete system DITSCAP. Obtain DAA approval of WLAN system.	X
Determine if the proposed SWLAN architecture fits into an approved DSWAG use case.	X
If SWLAN Architecture does not clearly fit the DSAWG approved architectures, then contact DISA to have the system design reviewed. Document DISA review of the system.	X
Submit a SIPRNet CAP package to the SCAO.	X
Comply with SCAO or DSAWG requirements for additional system documentation, testing, or security reviews.	X

Table 4-1. Connection Approval Steps for Wireless Connection to the SIPRNet

4.3.2 SWLAN Requirements

DSAWG and NSA have identified high-level requirements for the implementation of a SWLAN. These requirements are listed in *Table 4.2, SWLAN Requirements,* and serve as a minimum baseline and must be met by any proposed implementation. How these requirements will be met must be included in the package submitted to the SCAO. Depending on the operational environment, additional requirements may apply.

Category	Requirement
Environment	The SWLAN must be designed for use in any DOD environment. Use outside the United States must be approved by the host nation to ensure spectrum compliance.
Possession of SWLAN Components	Only personnel with the appropriate security clearance may possess the card.
Intrusion Detection	All traffic must pass through a Network based IDS. A wireless IDS/RF monitor should be used to detect active wireless or DoS attacks.
Local Security Policy	The SWLAN design and security procedures, including IP address management, must be documented in a local policy.
Lost, Stolen or Compromised Devices	The SWLAN must implement access filtering. The SA must set the system to deny network access to cards that are reported as lost, stolen, or compromised. Re-keying procedures must be established. A secondary means of verifying AP and Client compromise must be provided. For example, physical control of compromised devices or an ability to ensure that the compromised device is "zeroized."
Power Setting	Power settings must be set to the lowest power setting required for the desired coverage area.
EMCON	The SWLAN must comply with EMCOM requirements.
TEMPEST	Coordinate with the CTTA and comply with TEMPEST guidelines: 20 meters of inspectable and controllable space; 3 meters of separation between systems processing unclassified and classified data.
OPSEC	SecNet enabled devices must be used only in a controlled environment.
Cryptographic Re-keying	The SWLAN card must be re-keyed every 90 days and at the end of each mission.
Inventory Control	Tight inventory control of SWLAN components is required. SecNet PC cards and APs must be inventoried by serial number and/or MAC address.
Coalition Communication	Wireless communication between coalition members must occur in accordance with existing policy.
Back-up Communications	Back-up communication procedures should be established in case jamming or RF flooding occurs.

Table 4-2. SWLAN Requirements

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

The following table highlights the relevant policies and guidance for implementing a wireless infrastructure. These policies serve as required practices for DOD users and administrators using wireless networks.

Policy	Description
Wireless STIG	This STIG developed by DISA for the DOD is published as a tool to assist in improving the security of DOD wireless information systems and clients.
Secure Remote Computing STIG	This STIG developed by DISA for the DOD provides the requirements and guidance needed to ensure a secure remote access environment for users within the DOD.
Desktop Application STIG	This STIG developed by DISA for the DOD provides technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications on desktop workstations.
Network Infrastructure STIG	This STIG provides security considerations at the network level along with an acceptable level of risks and some guidelines for best network technical practices.
Wireless Security Framework	This guidance provides a common conceptual framework to assist the DOD in coordinating acquisition, development, architecture design, and implementation of 802.11 wireless infrastructures connected to the NIPRNet.
Secure Wireless LAN CONOPS	CONOPS describes the security requirements and architecture of a WLAN using SecNet 11 technology. The WLAN architecture is composed of new security components and technologies that can function in various military environments. https://powhatan.iiie.disa.mil/ (DOD PKI certificate required)
DODD 8100.2	Describes the use of commercial wireless devices, services, and technologies in the DOD Global Information Grid (GIG).
DODD 8500.1	Prescribes the use of a defense-in-depth approach.
DODI 8500.2	Implements policy; assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DOD information systems and networks under DODD 8500.1.
DOD Mobile Code Policy	Categorizes mobile code technologies and restricts their application within DOD based on their potential to cause damage if used maliciously.
PDS Guidebook	NAVSO P-5239-22: Protected Distribution System (PDS) Guidebook
CJCSI 6211.02B	This instruction establishes policy, responsibilities and a connection approval process for sub networks of the Defense Information System Network (DISN).

This page is intentionally left blank.

APPENDIX B. LIST OF ACRONYMS

AES	Advanced Encryption Standard
C&A	Certification and Accreditation
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DISAI	DISA Instruction
DISN	Defense Information System Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DODAAC	Department of Defense Activity Address Code
DDoS	Denial of Service
DSAWG	Defense Information System Network (DISN) Security Accreditation Working Group
FIPS	Federal Information Processing Standard
FSO	Field Security Operations
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
I&A	Identification and Authentication
IAM	Information Assurance Manager
IP	Internet Protocol
IPSEC	IP Security
LAN	Local Area Network
MAC	Media Access Control
NIC	Network Interface Card
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NSO	Network Security Officer
OS	Operating System
OUS&P	Outside United States & Possessions

PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PKI	Public Key Infrastructure
SA	System Administrator
SCI	Secure Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SRR	Security Readiness Review
SRRDB	SRR Database
SSAA	System Security Authorization Agreement
SSID	Service Set Identifier
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
USB	Universal Serial Bus
VCTS	Vulnerability Compliance Tracking System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WB	Wireless Bridge
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WMAN	Wireless Metropolitan Area network
WPA	Wireless Protected Access
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WWW	World Wide Web