Cisco 3220 Mobile Access Router Card
Cisco 3251 Mobile Access Router Card

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation
Version 1.5

September 23, 2004

© Copyright 2004 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 Introduction

1.1 *Purpose*

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 3220 and 3251 Mobile Access Router Cards. This security policy describes how the 3220 and 3251 Mobile Access Routers Cards (Hardware Version: 3.2; Firmware Version: 12.2(11r)YQ4) meet the security requirements of FIPS 140-2, and how to operate them in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the Cisco 3220 and 3251 Mobile Access Routers.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 *References*

This document deals only with operations and capabilities of the 3220 and 3251 Mobile Access Router Cards in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the 3220 and 3251 Mobile Access Router Cards and the entire 3200 series from the following sources:

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The 3200 Series product descriptions can be found at: http://www.cisco.com/en/US/products/hw/routers/ps272/index.html.
- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module

1.3 *Terminology*

In this document, the Cisco 3220 and 3251 Mobile Access Router Cards are referred to as the 3220 Router or 3251 Router (respectively), the router or routers, the module or modules, or the system or systems.

1.4 *Document Organization*

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- ♦ Vendor Evidence document
- ♦ Finite State Machine
- ♦ Module Software Listing
- ♦ Other supporting documentation as additional references

This document provides an overview of the Cisco 3220 and 3251 Mobile Access Routers and explains the secure configuration and operation of the module. This introduction section is

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

followed by Section 2, which details the general features and functionality of the 3220 and 3251 Mobile Access Router Cards. Section 3 specifically addresses the required configuration for the FIPS-Approved mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2 The Cisco 3220 and 3251 Mobile Access Router Cards

The Cisco 3220 and 3251 Mobile Access Routers Cards are high-performance cards in a compact form factor ideally suited for integration in vehicles. They offer secure data, voice and video communications, seamless mobility and interoperability across multiple wireless networks. The Cisco 3220 and 3251 Mobile Access Router Cards along with the other Network interface cards (such as FESMIC and SMIC) extend the edge of the IP network to a new frontier of Networks-in-Motion and facilitates new and exciting applications in the defense, public safety, homeland security, and commercial transportation markets. The Routers offer users the following benefits:

- Secure data, voice and video communications with seamless mobility across wireless networks independent of location or movement
- High performance in a compact, rugged design for use in vehicles
- Advanced IP services and interoperability through Cisco IOS Software

The Cisco 3220 and 3251 Mobile Access Router Cards leverage Cisco IOS software features including Mobile Networks, security, QoS, routing and management functionality to deliver comprehensive services for Networks-in-Motion. They provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements except for physical security for which it meets level 1 requirements. This section describes the general features and functionality provided by the Cisco 3220 and 3251 Mobile Access Router Cards.

2.1 The 3220 and 3251 Cryptographic Module

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

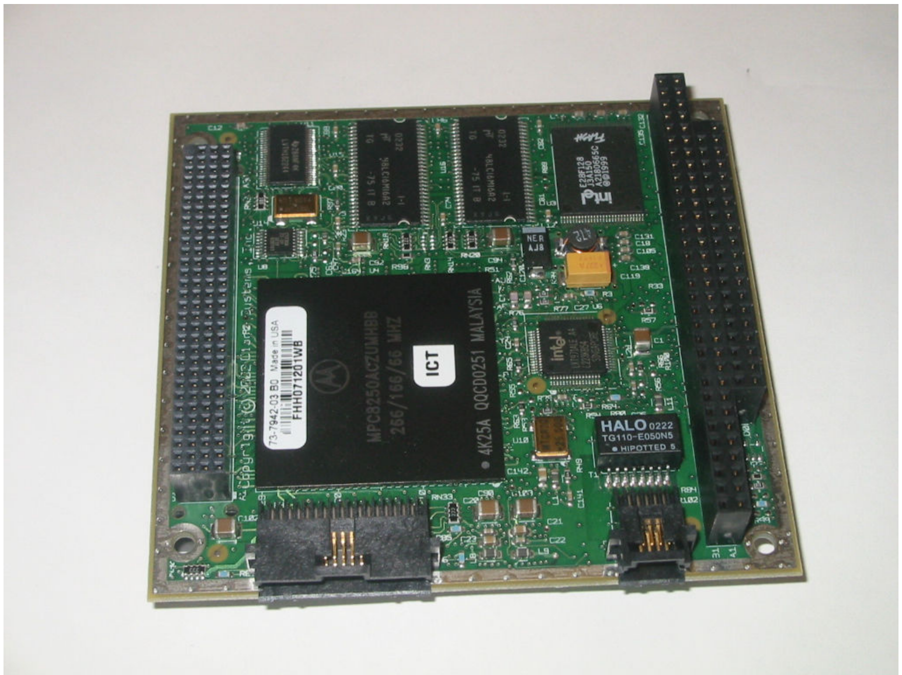

Figure 1 - The 3220 and 3251 Router

The 3220 and 3251 Routers are multi-chip embedded cryptographic modules. The cryptographic boundary is defined as the Mobile Access Router Card ("MARC"). The cryptographic boundary includes the PCI, ISA, and PC/104-Plus PCI connection interfaces between the MARC and other cards (such as the Serial Mobile Interface Card ("SMIC") or Fast-Ethernet Switch Mobile Interface Card ("FESMIC")), but the boundary does not include any other cards. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 3220 and 3251 Mobile Access Routers an ideal platform for building virtual private networks or outsourced dial solutions. The modules' RISC-based processor provides the power needed for the dynamic requirements of the remote branch office.

2.2 Module Interfaces

The Cisco 3220 and 3251 Routers feature a multifunctional header interface, which provides functionality to connect a console port, auxiliary ports, and system and network LEDs. The module also provides the ability to add network modules and other interface cards via the PC/104-Plus PCI interface. Network modules support a variety of serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity.

An NM is connected to the PC/104-Plus PCI bus interface. NMs interface directly with the processor, and cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The physical interfaces include the ISA interface which provides power to the module via the power card. The module also has an RS-232 connector for a console terminal for local system access. The router also has a multifunctional header interface which connects to system and network status LEDs, the console port and auxiliary port. Table 1 describes the LEDs:

LED	Indication	Description
MARC (In ROMMON)		
OK	S	Normal operation
LINK	S	Normal operation
ACT	OFF	Normal operation
MARC (During Boot-up)		
OK	B, S	Normal operation
LINK	S, OFF, S, OFF, S	F0/0 interface is Not Shutdown and is connected to another device
	S, OFF, S	F0/0 interface is Shutdown and is connected to another device
	S, OFF	F0/0 interface is not connected to another device
ACT	OFF, S, B	F0/0 interface is Not Shutdown and is connected to another device
	OFF, S, OFF	F0/0 interface is Shutdown and is connected to another device
	OFF	F0/0 interface is not connected to another device
MARC (In IOS)		
OK	S	Normal operation
LINK	S	F0/0 interface is connected to another device
	OFF	F0/0 interface is not connected to another device
ACT	OFF, B	F0/0 interface is Not Shutdown and is connected to another device
	OFF	F0/0 interface is Shutdown and/or is not connected to another device
SMIC (In DTE mode)		
ACT	B	A packet is transmitted or received via the Serial1 port
LINK	OFF	Date Set Ready (DSR), Data Carrier Detect (DCD), and Clear To Send (CTS) are not detected.
	S	Date Set Ready (DSR), Data Carrier Detect (DCD), and Clear To Send (CTS) are detected.
SMIC (In DCE mode)		
ACT	B	A packet is transmitted or received via the Serial1 port
LINK	OFF	Data Terminal Ready (DTR) and Request To Send (RTS) are not detected.
	S	Data Terminal Ready (DTR) and Request To Send (RTS) are detected.
FESMIC		
ACT	B	A packet is transmitted or received via the FESMIC port
LINK	OFF	Link state is “down”
	S	Link state is “up”

Table 1 – 3220 and 3251 LEDs and Descriptions

All of these physical ports are separated into the logical interfaces from FIPS 140-2 as described in the following table:

Router Physical Port	FIPS 140-2 Logical Interface
10/100 Base T Multifunctional Header PC/104-Plus PCI Interface	Data Input Interface

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Router Physical Port	FIPS 140-2 Logical Interface
10/100 Base T Multifunctional Header PC/104-Plus PCI Interface	Data Output Interface
10/100 Base T ISA interface Multifunctional Header PC/104-Plus PCI Interface	Control Input Interface
Multifunctional Header 10/100 Base T PC/104-Plus PCI Interface	Status Output Interface
ISA Interface	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

2.3 Roles and Services

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. Both roles are authenticated by providing a valid username and password. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode. A complete description of all the management and configuration capabilities of the Cisco 3220 and 3251 Mobile Access Router Cards can be found in the *Performing Basic System Management* manual and in the online help for the router.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See Section 3, *Secure Operation of the Cisco 3220 and 3251 Mobile Access Router*, for more information. If only integers 0-9 are used without repetition for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

2.3.1 Crypto Officer Role

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- **Configure the router**: define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions**: view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- **Manage the router**: log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- **Change Port Adapters**: insert and remove adapters in a port adapter slot.

2.3.2 User Services

A User enters the system by accessing the console port with a terminal program. The IOS prompts the User for their password. If the password is correct, the User is allowed entry to the IOS executive program. The services available to the User role consist of the following:

- **Status Functions**: view state of interfaces, state of layer 2 protocols, version of IOS currently running
- **Network Functions**: connect to other network devices (via outgoing telnet or PPP) and initiate diagnostic network services (*i.e.*, ping, mtrace)
- **Terminal Functions:** adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services**: display directory of files kept in flash memory

2.4 Physical Security

The router must be installed within an approved chassis. Such chassis are available from various resellers; please contact your Cisco distributor for more information. Console and auxiliary port connectors are provided on the router, and the power cable connection is provided on the power supply.

2.5 Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The module supports the following critical security parameters (CSPs):

#	CSP	Description	Storage

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

	Name		
1	CSP 1	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	DRAM (plaintext)
2	CSP 2	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
3	CSP 3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
4	CSP 4	Same as above	DRAM (plaintext)
5	CSP 5	Same as above	DRAM (plaintext)
6	CSP 6	Same as above	DRAM (plaintext)
7	CSP 7	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
8	CSP 8	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
9	CSP 9	The RSA private key. "crypto key zeroize" command zeroizes this key.	NVRAM (plaintext)
10	CSP 10	The key used to generate IKE skeyid during preshared-key authentication. "no crypto isakmp key" command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)
11	CSP 11	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
12	CSP 12	The RSA public key used to validate signatures within IKE. These keys are expired either when CRL (certificate revocation list) expires or 5 secs after if no CRL exists. After above expiration happens and before a new public key structure is created this key is deleted. This key does not need to be zeroized because it is a public key; however, it is zeroized as mentioned here.	DRAM (plaintext)
13	CSP 13	The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash.	NVRAM (plaintext)
14	CSP 14	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
15	CSP 15	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
16	CSP 16	The RSA public key of the CA. "no crypto ca trust <label>" command invalidates the key and it frees the	NVRAM (plaintext)

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

		public key label which in essence prevent use of the key. This key does not need to be zeroized because it is a public key.	
17	CSP 17	This key is a public key of the DNS server. Zeroized using the same mechanism as above. “no crypto ca trust <label>” command invalidate the DNS server’s public key and it frees the public key label which in essence prevent use of that key. This label is different from the label in the above key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
18	CSP 18	The SSL session key. Zeroized when the SSL connection is terminated.	DRAM (plaintext)
19	CSP 19	The ARAP key that is hardcoded in the module binary image. This key can be deleted by erasing the Flash.	Flash (plaintext)
20	CSP 20	This is an ARAP user password used as an authentication key. A function uses this key in a DES algorithm for authentication.	DRAM (plaintext)
21	CSP 21	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued.	NVRAM (plaintext)
22	CSP 22	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM (plaintext)
23	CSP 23	The RSA public key used in SSH. Zeroized after the termination of the SSH session. This key does not need to be zeroized because it is a public key; However, it is zeroized as mentioned here.	DRAM (plaintext)
24	CSP 24	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)
25	CSP 25	This key is used by the router to authenticate itself to the peer. The key is identical to #22 except that it is retrieved from the local database (on the router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
26	CSP 26	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
27	CSP 27	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
28	CSP 28	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

29	CSP 29	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
30	CSP 30	The RADIUS shared secret. This shared secret is zeroized by executing the “no” form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM (plaintext)
31	CSP 31	The TACACS+ shared secret. This shared secret is zeroized by executing the “no” form of the TACACS+ shared secret set command.	NVRAM (plaintext), DRAM (plaintext)

Table 3 – Critical Security Parameters

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Table 4.

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

SRDI/Role/Service Access Policy	Security Relevant Data Item	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22	CSP 23	CSP 24	CSP 25	CSP 26	CSP 27	CSP 28	CSP 29	CSP 30	CSP 31
Role/Service																																
User role																																
Status Functions																																
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r		r	r	r	r	r	r				
Terminal Functions																																
Directory Services																																
Crypto-Officer Role																																
Configure the Router														r w d						r w d		r w d				r w d						
Define Rules and Filters																																
Status Functions																																
Manage the Router		d																			r w d	r w d	r w d		d			r w d	r w d	r w d	r w d	r w d
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w	r w d	r w d					r w d	r w		r w d					
Change WAN Interface Cards																																

Table 4 – Role and Service Access to CSPs

© Copyright 2004 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The module supports DES (only for legacy systems), 3DES, DES-MAC, TDES-MAC, AES, SHA-1, HMAC SHA-1, MD5, MD4, HMAC MD5, Diffie-Hellman, RSA (PKCS#1, for digital signatures and encryption/decryption (for IKE authentication)) cryptographic algorithms. The MD5, HMAC MD5, and MD4 algorithms are disabled when operating in FIPS mode.

The module supports three types of key management schemes:

1. A symmetric manual key exchange method. DES, 3DES, and AES keys and HMAC-SHA-1 keys are exchanged manually and entered electronically.
2. The Internet Key Exchange method with support for exchanging pre-shared keys manually and entering electronically.
    - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, 3DES or AES keys.
    - The pre-shared key is also used to derive HMAC-SHA-1 key.
3. The Internet Key Exchange with RSA-signature authentication.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol.

Key Zeroization:
All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 3 for information on methods to zeroize each key and CSP.

2.6 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Power-up tests

Firmware integrity test
RSA signature KAT (both signature and verification)
DES KAT
TDES KAT
AES KAT
SHA-1 KAT
PRNG KAT
Power-up bypass test
Diffie-Hellman self-test
HMAC SHA-1 KAT

© Copyright 2004 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Conditional tests

- Conditional bypass test
- Pairwise consistency test on RSA signature
- Continuous random number generator tests

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3 Secure Operation of the Cisco 3220 and 3251 Mobile Access Routers

The Cisco 3220 and 3251 Mobile Access Router Cards meet all of the Level 2 requirements for FIPS 140-2 except for physical security for which it meets Level 1 requirements. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Initial Setup

1. Only a Crypto Officer may add and remove port adapters.
2. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal

no service password-recovery

end

show version
```

   NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.2(11r)YQ4 is the only allowable image; no other image may be loaded.
2. The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
config-register 0x0101
```

3. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
line con 0

password [PASSWORD]

login local
```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6. The Crypto Officer shall not assign a command to any privilege level other than its default.
7. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
8. If the Crypto Officer loads any IOS image onto the router, this will put the router into a non-FIPS mode of operation.

3.3 IPSec Requirements and Cryptographic Algorithms

1. There are two types of key management method that are allowed in FIPS mode: Internet Key Exchange (IKE) and IPSec manually entered keys.
2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
    - ah-sha-hmac
    - esp-des
    - esp-sha-hmac
    - esp-3des
    - esp-aes
3. The following algorithms are not FIPS approved and should be disabled:
    - MD-4 and MD-5 for signing
    - MD-5 HMAC

3.4 Protocols

1. All SNMP operations must be performed within a secure IPSec tunnel.

3.5 Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.
2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms.

© Copyright 2004 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

CISCO EDITOR'S NOTE: You may now include all standard Cisco information included in all documentation produced by Cisco. Be sure that the following line is in the legal statements at the end of the document:

> *By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.*

© Copyright 2004 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.