



Network Security Checklist - IDS

Version 7, Release 1.1

20 November 2007

Developed by DISA for the DOD

UNCLASSIFIED

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

NET0230 **V0003012 CAT I** **Communications devices are not password protected.**

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all communications devices are password protected.

Vulnerability Discussion The lack of a password protection for communications devices provides anyone access to the device, which opens a backdoor opportunity for intruders to attack and manipulate or compromise network resources. Vendors and programmers often leave methods of gaining access to a device that is outside the normal means of access. These backdoors or hidden userids are well known and are extremely dangerous if left active.

Checks

NET Password Protection

Interview the network administrator and attempt to logon to several devices.

Default Finding Details Communications devices are not password protected in accordance with DISA requirements.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Password Protection

Ensure all communication devices are in compliance with password policy.

Notes:

NET0340 **V0003013 CAT II** **Warning banner compliance to 8500.2 ECWM-1.**

8500.2 IA Control: ECWM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.

Vulnerability Discussion Failure to display the required login banner prior to logon attempts will limit the sites ability to prosecute unauthorized access and also presents the potential to give rise to criminal and civil liability for systems administrators and information systems managers. Not displaying the proper banner will also hamper the sites ability to monitor device usage.

Checks

NET Warning Banners

Have the network administrators sign onto each managed network device to ensure the DoD approved warning banners are displayed before the password prompt and after a correct login.

Default Finding Details DOD approved warning banners, adhering to Appendix C of the Network Infrastructure STIG, are not displayed on network managed devices.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Warning Banner

Display the approved DOD login banner prior to a login attempt on all network devices allowing Telnet, File Transfer Protocol (ftp), or Hyper Text Transfer Protocol (http) access.

Notes: