

Open or Unkown Status

Total of All System Findings With this Status: 125

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
COD 7	There are an excessive number of user accounts assigned to administrator security groups	Unknown	Unknown	11/1/2003		IGIC-03
COD 8	There are no adequate controls in place to limit an individual's access to the COD system. Controls around granting user access to the COD system are not operating	Unknown	Unknown	11/1/2003		IGIC-03
COD 10	There is no formal procedure or requirement in place for COD to periodically monitor user accounts for improper access privileges	Unknown	Unknown	11/1/2003		IGIC-03
COD 12	The disaster recovery plan does not address critical data files	Unknown	Unknown	11/1/2003		IGIC-03
COD 13	The disaster recovery plan does not address procedure to be followed when the data service center cannot receive or transmit data	Unknown	Unknown	11/1/2003		IGIC-03

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
COD 14	The disaster recovery plan does not address procedures for regeneration of the system files	Unknown	Unknown	11/1/2003		IGIC-03
COD 15	The disaster recovery plan does not address how the plan will be distributed to the appropriate personnel	Unknown	Unknown	11/1/2003		IGIC-03
COD 16	Program change controls: The release document, which serves as a summarized planning document with explanations of the proposed changes, did not contain any information related to the change selected for testing	Unknown	Unknown	11/1/2003		IGIC-03
DLOS 1	Windows NT and UNIX security audits are not fully documented	Open	Concur			2002 risk assessment
DLOS 2	Computer security incidents continue to be tracked and recorded manually	Open	Unknown			2002 risk assessment

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 39	Database Link Password Encryption/Login Encryption Parameter Settings are not Secure IG Action Memo noted that the "DBLINK_ENCRYPT_LOGIN" or the "ORA_ENCRYPT_LOGIN" parameter settings is not configured to encrypt stored passwords or encrypt users passwords when users connect to the database...	Unknown	Concur		12/15/2003	IG
DLSS 40	User Account Granted the CONNECT Default Role IG Action Memo: noted that numerous user accounts are granted the CONNECT Default Role for database connections...	Unknown	Concur		12/15/2003	IG
DLSS 41	User Accounts Assigned to the Default System Tablespace IG Action Memo: noted that certain user accounts are assigned the default tablespace of SYSTEM...	Unknown	Concur		12/15/2003	IG
DLSS 44	Statement Permissions Granted to User Accounts IG Action Memo: identified four SQL Server databases (RCC = 1) that had granted "STATEMENT" permissions to various user accounts...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 47	Account LockoutIG Action Memo: noted that all 10 servers tested at the RCC have not configured settings to lock out accounts after a specified number of unsuccessful logon attempts...	Unknown	Concur		12/15/2003	IG
DLSS 49	Disabling LANMAN Authentication on Domain ControllersIG Action Memo: noted that domain controllers at the RCC were not configured to disable LANMAN user authentication over the network... NOTE: ACS cannot disable LANMAN authenticataion or domain controllers because it disrupts clustering capabilities.	Unknown	Concur		12/15/2003	IG
DLSS 52	Act as Part of Operating SystemIG Action Memo: noted that on many servers tested (RCC = 3), the Administrators or Everyone user group had permission to perform this function...	Unknown	Concur		12/15/2003	IG
DLSS 54	Permissions on Memory Dump FilesIG Action Memo: noted that on one server at the RCC, the Everyone user group had full access to the memory dump file...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 55	Excessive Permissions on System Files and DirectoriesIG Action Memo: noted that on most servers tested at the RCC and EDNet, the Everyone user group had full access to the following critical system files and directories...: NOTE: ACS cannot address without disrupting critical production	Unknown	Concur		12/15/2003	IG
DLSS 56	World Writable FilesIG Action Memo: noted that a number of servers (RCC = 2) contained files that were assigned permissions allowing any user to access certain files and directories, modify their contents, and execute various functions. We also identified world writeable configuration files in the /etc directory that provide for any process to have the ability to alter the configuration of the system seizing unauthorized resources or denying resources to authorized users...NOTE: files created by VMS.	Unknown	Concur		12/15/2003	IG
DLSS 57	Excessive Set-User ID/Set-Group ID (SUID/SGID) FilesIG Action Memo: identified 5 servers at the RCC that contained excessive files with imbedded SUID and SGID permissions...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 58	Use of hosts.equiv and rhosts files IG Action Memo: identified several servers (RCC = 3) containing hosts.equiv and rhosts files which indicates that trust relationships have been established with other systems on the network. In addition, we noted that these files contain a root user account, ...	Unknown	Concur		12/15/2003	IG
DLSS 59	Firmware Security Mode and Password are not Utilized IG Action Memo: identified two Sun Solaris servers at the RCC that have not enabled the firmware security mode and password (EEPROM) setting... NOTE: Not going to close	Unknown	Concur		12/15/2003	IG
DLSS 60	System Files and Directories not Owned by Root IG Action Memo: identified three servers at the RCC that contain key system files and directories (e.g., /etc, /dev, /bin, and /usr/etc) that are not owned by root... NOTE: Not going to close	Unknown	Concur		12/15/2003	IG
DLSS 61	Unique Universal Identification Code (UIC) for all User Accounts IG Action Memo: noted that the majority of online user accounts were assigned the same UIC, which results in a loss of individual accountability within DLSS...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 62	Authorization and Access Control List (ACL) Event Classes are not Enabled IG Action Memo: noted that the Authorization and ACL event classes are not enabled to capture security related ... NOTE: Not going to close	Unknown	Concur		12/15/2003	IG
DLSS 63	EnableForcedLogoffIG Action Memo: discovered that most servers (RCC = 2 and VDC = 10) had not configured this setting to allow Administrators to force users	Unknown	Concur		12/15/2003	IG
DLSS 64	AutodisconnectIG Action Memo: discovered that most servers (RCC = 2 and VDC = 7) had not configured this setting to allow Administrators to disconnect users	Unknown	Unknown		12/15/2003	IG
DLSS 65	IOS – Defining a Telnet Access Control List (ACL)IG Action Memo: noted that the routers at the RCC have not adequately defined an ACL to limit the number of Telnet (Virtual Type Terminal (VTY) ports) connections and corresponding IP addresses that are able to log onto the router..	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 66	IOS – Exec TimeoutIG Action Memo: noted that routers at RCC have not defined IOS – Exec Timeout parameter on all console and auxiliary interfaces...	Unknown	Concur		12/15/2003	IG
DLSS 67	IOS – TCP Keepalive ServiceIG Action Memo: noted that the routers at the RCC have not enabled this service to terminate connections if the host on the other end of an idle connection has been lost...	Unknown	Concur		12/15/2003	IG
DLSS 68	IOS – No IP Source RouteIG Action Memo: noted that two routers at the RCC have not defined the IOS – No IP Source Route parameter to mitigate against well known Denial of Service attacks associated with the service...	Unknown	Concur		12/15/2003	IG
DLSS 69	IOS – No IP Proxy Address Resolution Protocol (ARP)IG Action Memo: noted that the routers at the RCC have not implemented this parameter to mitigate against trust relationships created by this service... NOTE: ACS needs further testing to implement	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 70	IOS – Network Time Protocol (NTP) Server/SourceIG Action Memo: noted that the routers at the RCC have not defined the IOS – NTP Server/Source parameter that is required for communication and time synchronization with other NTP servers...	Unknown	Concur		12/15/2003	IG
DLSS 71	IOS – VTY Transport TelnetIG Action Memo: noted that the routers at the RCC have not defined this parameter to ensure that only telnet connections are allowed for remotely accessing routers and will ensure that other unsecured protocols (e.g. rlogin, WWW) can	Unknown	Concur		12/15/2003	IG
DLSS 72	IOS – Logging Trap InfoIG Action Memo: noted that most routers at the RCC have not defined this parameter to allow administrators to configure the severity level of messages that will generate SNMP	Unknown	Concur		12/15/2003	IG
DLSS 73	IOS – No IP Bootp Server IG Action Memo: noted that most routers at the RCC have not defined this parameter to disable the Bootp service in accordance with vendor recommended settings...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 74	IOS – Service StampsIG Action Memo: noted that the routers at the RCC had not enabled this service to ensure that logging messages are timestamped...	Unknown	Concur		12/15/2003	IG
DLSS 75	Insufficient Disk CapacityIG Action Memo: noted that a number of servers (RCC = 1,) were experiencing disk utilization rates greater than 90 percent and therefore may not have sufficient disk capacity to perform normal	Unknown	Concur		12/15/2003	IG
DLSS 76	Allocate FloppiesIG Action Memo: noted that on the majority of servers tested (RCC = 7,) this setting was not configured to restrict use of the floppy drive to users logged onto the console interface...	Unknown	Concur		12/15/2003	IG
DLSS 77	Allocate CDROMSIG Action Memo: noted that on the majority of servers tested (RCC = 7,) this setting was not configured to restrict use of the CDROM drive to users logged onto the console interface...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 78	AutoAdminLogonIG Action Memo: discovered that on most servers tested (RCC = 6), this setting was not configured to prevent unauthorized users from bypassing Windows NT authentication processes and gaining administrator privileges...	Unknown	Concur		12/15/2003	IG
DLSS 79	DontDisplayLastUserNameNote: this same vulnerability is listed twice in report.IG Action Memo: noted that on most servers tested (RCC = 10.), this setting was not configured to prevent displaying the last user's account name during subsequent logon sessions...	Unknown	Concur		12/15/2003	IG
DLSS 81	LanMan (LM) Hash System Vulnerability IG Action Memo: identified seven servers at the RCC that have enabled the LM hash setting for user authentication. LM uses a weak encryption scheme and passwords can be broken in a very short period of time, allowing an attacker to gain access to the system. ...	Unknown	Concur		12/15/2003	IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 84	Audit Logging does not utilize Audit and Alarm Access Control Entries (ACE)IG Action Memo: noted that the audit function within DLSS is not configured to utilize Audit and Alarm ACE's to track user activity and identify unauthorized attempts to modify log files...	Unknown	Concur		12/15/2003	IG
DLSS 85	System Parameters do not comply with Vendor Recommended SettingsIG Action Memo: noted that the DLSS security system parameter "RMS_FILEPROT" is configured with the default file protection setting (64,000.. also noted that the "SECURITY POLICY" parameter (7) is configured to not notify security operator terminals in the event that a system intrusion has been identified...	Unknown	Concur		12/15/2003	IG
DLSS 86	No means of tracking user compliance of annual security awareness training	Unknown	Unknown	11/13/2003		C&A
DLSS 87	Rules of behavior have not been established to delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior.	Unknown	Closed	11/13/2003	1/19/2004	C&A

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 88	There was no evidence documenting whether or not public access was allowed to DLSS.	Open	Unknown			2002 risk assessment
DLSS 92	Statistical analysis to spot abnormal activity patterns that may indicate an attack is not performed proactively. Applies to	Open	Concur			2002 risk assessment
DLSS 97	Technical controls to ensure appropriate security controls are specified, designed into and accepted in the application in accordance with NIST guidance are not completed. NOTE: completed for utica t3, bakersfield t4; ongoing for dallas t1, southgate t1	Open	Concur			2002 risk assessment
DLSS 108	Access request forms are not signed off by the appropriate manager	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 109	Access request forms not complete or having pages missing	Unknown	Unknown	11/1/2003		IGIC-03

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 110	Actual access rights differ from the access rights listed on the request forms	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 111	47 percent of the separated employees tested did not have their eCRM account removed, and that 27 percent of the separated employees did not have their green screen account removed	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 112	Access-rights reviews do not include an evaluation of current user's access rights to the system.	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 113	Audit trails: No functionality in place to track the activities performed by system administrators	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 114	There is no documented policy or procedure that serves as a guideline for the process of identifying, evaluating, and implementing security patches for the infrastructure that supports DLSS.	Unknown	Unknown	11/1/2003		IGIC-03

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
DLSS 115	There is no formal tracking mechanism for security incidents, their status, and their resolution	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 116	The DLSS security plan does not contain documented procedures that define the monitoring process for DLSS' compliance with FSA's security regulations and guidelines.	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 117	There is a lack of appropriate segregation of duties over the change management process for DLSS.	Unknown	Unknown	11/1/2003		IGIC-03
ECB 21	The risk assessment referenced is over a year old and was directed towards a mainframe system, not eCBS.	Open	Noncur			C&A Precert
ERMS 1	The configuration management plan does not contain current version numbers of system software	Open	Unknown	11/17/2003		C&A

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
ERMS 2	The configuration management plan does not demonstrate that system software has been properly licensed	Open	Unknown	11/17/2003		C&A
ERMS 4	Warning banners are not displayed, as required, on every login screen	Open	Unknown	11/17/2003		C&A
ERMS 5	Passwords do not meet complexity criterion	Open	Unknown	11/17/2003		C&A
ERMS 6	There is no separation of duties	Open	Unknown	11/17/2003		C&A
ERMS 7	There is no designated system owner	Open	Unknown	11/17/2003		C&A

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
ERMS 8	There are no documented procedures describing creation of emergency passwords	Open	Unknown	11/17/2003		C&A
ERMS 10	Physical access to Richmond and St. Paul facilities not adequately tested	Open	Concur			2002 risk assessment
NSLDS 7	The password guidelines documented in the security plan do not fully comply with those required by FSA policy and the Department of Education Handbook for Information Technology Security	Open	Unknown	11/1/2003		IGIC-03
NSLDS 8	The current process to remove terminated employee accounts from the NSLDS application is not operating effectively	Open	Unknown	11/1/2003		IGIC-03
SAIG 1	The configuration management plan does not demonstrate that system software has been properly licensed	Unknown	Unknown	11/17/2003		C&A

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
SAIG 2	Group users IDs are not limited to an "as necessary" basis	Unknown	Unknown	11/17/2003		C&A
SAIG 4	Users are not periodically recertified	Open	Unknown			2002 risk assessment
SAIG 5	There is no formal confirmation of the new employees acknowledging an understanding of the security awareness guidelines	Unknown	Unknown	11/1/2003		IGIC-03
SAIG 6	There are no yearly security awareness reeducation rebriefs taking place as discussed in the SAIG and VDC security manual	Unknown	Unknown	11/1/2003		IGIC-03
SAIG 7	There are no formal policies and procedures for conducting periodic reviews of user access privileges for SAIG employees, as well for developers working at NCS Pearson (who have access to SAIG)	Unknown	Unknown	11/1/2003		IGIC-03

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
SAIG 8	There are no formal policies or procedures for conducting periodic reviews of user access privileges for the Mainframe, Unix, and Windows NT environments	Unknown	Unknown	11/1/2003		IGIC-03
VDC 70	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server. (Unix, IP Address 4.20.14.31, 4.20.14.252) (Scan finding 165, 176)	Open	Unknown			
VDC 71	While performing procedures at the RECC, VC, and on Ednet, we noted that network and system administrators are informally performing reviews of certain network device and system audit logs but those procedures are not formally documented.	Open	Unknown			IGIC-03
VDC 72	We identified several servers (VDC = 1 and EDNet = 2) that have configured the Network File System (NFS) mount to provide access to all users. The NFS mount should be restricted to authorize users since an attacker could possibly mount the share and read files on the	Open	Unknown			IGIC-03

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 1	<p>· The VDC and EDNet system security plans identified broad policies for technical security controls but the specific procedures that are needed to enforce the policies have not been defined within the system security plans. For instance, the security plan specifies the minimum password requirement for all users but not identify the procedures of how this policy will be enforced on all platforms. We also noted that the system security plans did not address the specific responsibilities for system administrators, network administrators and database administrators in the following areas:</p> <p>1) enforcing complex password policies for all accounts; 2) removing all default user accounts and passwords; 3) maintaining all host servers and network devices with the required system security patches and system updates to eliminate common vulnerabilities and exposures; 4) periodically reviewing the security settings of host servers, databases, and network devices for security weaknesses; 5) administration of firewalls, databases, and other network devices; 6) establishing formal logging procedures and periodic review of audit logs for system administering network administrators and database administrators; and 7) system monitoring and incident response procedures for administrators.</p>	Open	Concur	11/7/2003		IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 3	Based on our review of the Department's internal "Risk Assessment Reports," program officials represent that all mission critical systems have controls to ensure that all employees receive mandatory periodic computer security awareness and training. During our review of the Principal Office's security awareness and specialized training programs, we noted that contractors supporting Department mission critical systems at the RCC, VDC, and on EDNet had not received the required computer security awareness training and specialized computer security training sponsored by the Department.	Open	Concur	11/7/2003		IG-Audit
VDC 5	We identified many servers (VDC = 98 and EDNet = 11) providing telnet services used for remote administration capabilities. Telnet service does not encrypt username, passwords, or transmitted data and is therefore vulnerable to sniffer attacks	Open	Concur			IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 6	We identified many servers (RCC = 12, VDC = 8, and EDNet = 11) using trust-based services such as "Rlogin" and "Rshell" which are vulnerable to well-known IP spoofing attacks that allow an attacker to execute commands from a trusted host. In addition, "Rlogin" passwords are transmitted in clear text and are therefore vulnerable to an attacker gaining passwords through sniffing activities.	Open	Concur			IG-Audit
VDC 7	We discovered many servers at the VDC using a version of SSH server that allows an attacker to use brute force techniques to determine usernames and passwords without this activity being logged by a	Open	Unknown			IG-Audit
VDC 8	We identified many servers (VDC = 27 and EDNet = 4) using a version of Apache web server, that is susceptible to buffer overflow attacks, which could allow an attacker to view the Apache password file.	Open	Unknown			IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 9	We identified many servers (RCC = 4 and VDC = 14) that are using a version of Sendmail, which is susceptible to several well-known vulnerabilities, such as providing an attacker with an opportunity to corrupt certain databases or Denial of Service attacks.	Open	Unknown			IG-Audit
VDC 10	We identified several servers (VDC = 1 and EDNet = 2) that have configured the Network File System (NFS) mount to provide access to all users. The NFS mount should be restricted to authorize users since an attacker could possibly mount the share and read files on the	Open	Unknown			IG-Audit
VDC 11	On most Oracle databases tested (VDC = 5 and EDNet = 2), we noted that auditing for system events is not enabled and the Audit Trail Table is not defined to its own system table space to avoid possible storage capacity limitations. Oracle auditing can be set to log audit data to the database or operating system	Open	Concur			IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 12	On most Oracle databases tested (VDC = 7, RCC = 1, and EDNet = 3), we noted that the "DBLINK_ENCRYPT_LOGIN" or the "ORA_ENCRYPT_LOGIN" parameter settings is not configured to encrypt stored passwords or encrypt users passwords when users connect to the database. Unencrypted passwords are vulnerable to an attacker gaining passwords through sniffing activities.	Open	Concur	11/10/2003		IG-Audit
VDC 14	We noted that the routers at the RCC and the VDC have not adequately defined an ACL to limit the number of Telnet (Virtual TypeTerminal (VTY) ports) connections and corresponding IP addresses that are able to log onto the router. We noted that certain Telnet ACLs permit access from an entire class of IP addresses.	Open	Concur	11/10/2003		IG-Audit
VDC 15	We noted that two routers at the VDC have not defined the "enable secret" parameter which uses a strong, one-way encryption algorithm to protect system passwords. This parameter setting should be used in place of the "enable password" command, which does not adequately protect system passwords.	Open	Concur	11/10/2003		IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 17	We noted that the routers at the RCC and the VDC have not enabled this service to terminate connections if the host on the other end of an idle connection has been	Open	Concur	11/10/2003		IG-Audit
VDC 18	We noted that the IOS – Logging Buffered parameter had not been implemented on most routers to ensure that routers will store logged messages in a memory buffer and to assist in resolving network connectivity problems.	Open	Concur	11/10/2003		IG-Audit
VDC 19	We noted that the routers at the RCC, VDC, and one router on EDNet have not defined the IOS – NTP Server/Source parameter that is required for communication and time synchronization with other NTP servers.	Open	Unknown			IG-Audit
VDC 20	We noted that the routers at the RCC and VDC have not defined this parameter to ensure that only telnet connections are allowed for remotely accessing routers and will ensure that other unsecured protocols (e.g. rlogin, WWW) can	Open	Concur	11/10/2003		IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 21	We noted that one router at the VDC has not defined IOS – No Finger Service parameter to disable the finger service in accordance with vendor recommended settings.	Open	Unknown			IG-Audit
VDC 22	We noted that most routers at the RCC and the VDC have not defined this parameter to disable the Bootp service in accordance with vendor recommended settings.	Open	Unknown			IG-Audit
VDC 23	We noted that the routers at the VDC had not enabled this service so that the Cisco routers can send their log messages to a Unix-style syslog server.	Open	Concur	11/10/2003		IG-Audit
VDC 24	We noted that the routers at the RCC and the VDC had not enabled this service to ensure that logging messages are timestamped.	Open	Concur	11/10/2003		IG-Audit
VDC 27	We noted that on most servers tested (RCC = 10 and VDC = 8), Administrators had permission to perform these functions.	Open	Concur	11/10/2003		IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 29	We discovered that on most servers tested (RCC = 6 and VDC = 7), this setting was not configured to prevent unauthorized users from bypassing Windows NT authentication processes and gaining administrator privileges.	Open	Concur			IG-Audit
VDC 30	We noted that on most servers tested (RCC = 10, VDC = 2, and EDNet = 10), this setting was not configured to prevent displaying the last user's account name during subsequent logon sessions. Providing a user account name can assist an attacker in gaining unauthorized access to critical resources.	Open	Concur			IG-Audit
VDC 32	We identified two HP-UX servers at the VDC where the number of system users exceeds the number of authorized users in accordance with the software license agreement.	Open	Unknown			IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 33	We noted that a number of servers (RCC = 2, VDC = 5, and EDNet = 4) contained files that were assigned permissions allowing any user to access certain files and directories, modify their contents, and execute various functions. We also identified world writeable configuration files in the /etc directory that provide for any process to have the ability to alter the configuration of the system seizing unauthorized resources or denying resources to authorized users. Excessive permissions may allow an unauthorized person to reconfigure critical system files and compromise the integrity of the operating system.	Open	Unknown			IG-Audit
VDC 34	We noted that a number of servers (RCC = 1, VDC = 10, EDNet = 1) were experiencing disk utilization rates greater than 90 percent and therefore may not have sufficient disk capacity to perform normal logging functions. Consequently, an attacker can force the log file to overflow and gain access to critical systems files without being detected by logging mechanisms.	Open	Concur			IG-Audit

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 35	We identified several servers (RCC = 3 and VDC = 2) containing hosts.equiv and rhosts files which indicates that trust relationships have been established with other systems on the network. In addition, we noted that these files contain a root user account, which may allow an attacker to gain unauthenticated access to other trusted systems with administrator privileges.	Open	Concur			IG-Audit
VDC 36	We identified several servers (VDC = 3 and EDNet = 3) that contain duplicate user IDs that may allow a system user to masquerade unauthorized activity.	Open	Concur			IG-Audit
VDC 37	We identified two servers at the VDC that contain shadow files that do not include all user account passwords from the "passwd" file listing. User accounts and passwords not included in shadow files are vulnerable for exploitation since the passwords are seen by all accounts and can be downloaded	Open	Concur			IG-Audit
VDC 39	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server. (IP Address: 4.20.2.240)	Open	Concur	10/30/2003		IG-Memo

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 42	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server. (IP Address 4.20.14.238)	Open	Concur	10/30/2003		IG-Memo
VDC 45	19 Windows NT Servers that utilize an outdated version of Compaq Web Management Server (CWMS),....	Open	Concur	10/30/2003		IG-Memo
VDC 46	19 Windows NT Servers that utilize an outdated version of Compaq Web Management Server (CWMS),....	Open	Concur	10/30/2003		IG-Memo
VDC 49	Disaster recovery exercises do not adequately test contingency plan viability and recovery team preparedness.	Unknown	Unknown			IG
VDC 50	Planning activities do not ensure that IT contingency plans are current and complete	Unknown	Unknown			IG

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 51	The Department has not established an effective coordination of IT contingency planning issues associated with complex system interfaces and interdependencies	Unknown	Unknown			IG
VDC 52	The configuration management plan does not state that system releases must be tested and debugged in a dedicated, controlled environment	Unknown	Unknown	9/11/2003		C&A
VDC 53	The configuration management plan does not require that software patches are tested	Unknown	Unknown	9/11/2003		C&A
VDC 54	Telnet, which has many known security issues, is currently deployed in the VDC environment	Unknown	Unknown	9/11/2003		C&A
VDC 55	Security awareness training and education does not meet federal guidelines	Unknown	Unknown	9/11/2003		C&A

<i>System Name</i>	<i>Finding</i>	<i>Status</i>	<i>Concur/Nonconcur</i>	<i>Date Reported</i>	<i>Date Closed</i>	<i>Sources</i>
VDC 58	Strengthen intrusion detection system--strengthen response to internal activity	Unknown	Unknown			IG
VDC 59	Strengthen intrusion detection system--adjust monitoring activities	Unknown	Concur			2002 IG GISRA
VDC 60	Address SNMP vulnerabilities--investigate community of interest adjustments	Unknown	Unknown			2002 IG GISRA