

Air Force DoDIIS Infrastructure (AFDI) Requirements Matrix

Versions (1.0, 1.1, 2.0, 2.x)

Document Release 1.0.1

10 August 00

Table of Contents

1.0	SYSTEM FUNCTIONS.....	4
1.1	CONSOLE WINDOW FUNCTION.....	4
1.2	SYSTEM SUPPORT FUNCTION.....	4
1.3	WEB INTERFACE FUNCTION.....	4
1.4	WINDOWING ENVIRONMENT FUNCTION.....	4
1.5	SCREEN LOCK FUNCTION.....	5
1.6	DEADMAN FUNCTION.....	5
1.7	DESKTOP MANAGER FUNCTION.....	6
1.8	DATABASE ACCESS AND FUNCTIONALITY.....	6
1.9	FUNCTIONAL TIMING REQUIREMENTS.....	7
1.10	AVAILABILITY.....	8
2.0	USER FUNCTIONS AND UTILITIES.....	9
2.1	PASSWORD TOOL FUNCTION.....	9
2.2	CHANGING PASSWORD FUNCTION.....	9
2.3	PRINTED OUTPUT FUNCTION.....	9
2.4	SECURE EMAIL FUNCTION.....	10
2.5	PING FUNCTION.....	10
2.6	PRINT STATUS FUNCTION.....	10
2.7	USER CREDENTIALS FUNCTION.....	11
3.0	SYSTEM ADMINISTRATION.....	11
3.1	PRINTING.....	11
3.2	PERMISSIONS FUNCTION.....	12
3.3	PROCESSES FUNCTION.....	12
3.4	NETWORK STATISTICS FUNCTION.....	13
3.5	TOOLS FUNCTION.....	13
3.6	SHELL FUNCTION.....	13
3.7	HOST CREDENTIALS FUNCTION.....	13
3.8	DISK SPACE FUNCTION.....	13
3.9	PERFORMANCE MANAGEMENT FUNCTION.....	14
3.10	HOST MAINTENANCE FUNCTION.....	14
3.11	PROTOCOL MAINTENANCE FUNCTION.....	15
3.12	PROTOCOL LISTER.....	15
3.13	NETWORK SERVICES FUNCTION.....	15
3.14	REMOTE DISTRIBUTION (RDIST) FUNCTION.....	15
3.15	NETWORK TIME PROTOCOL (NTP) FUNCTION.....	15
3.16	DOMAIN NAME SERVICE (DNS) FUNCTION.....	16
3.17	PRINTER DATABASE FUNCTION.....	16
3.18	HOST SERVICES FUNCTION.....	16
3.19	PERIPHERALS FUNCTION.....	16
3.20	SESSIONS FUNCTION.....	16
3.21	ACCOUNT MAINTENANCE FUNCTION.....	17
3.22	ACCOUNT INFORMATION FUNCTION.....	17
3.23	REBOOT FUNCTION.....	17
3.24	ALERT FUNCTION.....	17
3.25	PROCESS MANAGEMENT FUNCTION.....	17
3.26	ALERT MESSAGES FUNCTION.....	17
3.27	SEGMENTATION FUNCTION.....	18
3.28	INSTALLATION & CONFIGURATION FUNCTION.....	18
3.29	AUTOMATED INSTALLATION FUNCTION.....	19

4.0	SECURITY MANAGEMENT	20
4.1	SECURITY ADMINISTRATION FUNCTION	20
4.2	ACCOUNTABILITY	20
4.3	AUDIT FUNCTION	21
4.4	LOGGING AND SECURITY AUDIT FUNCTION	22
4.5	SECURITY AND CONFIDENTIALITY REQUIREMENTS	25
4.6	CENTRALIZED LOG/AUDIT SUPPORT SUBSYSTEM (CLASS) FUNCTION	25
4.7	TRUSTED FACILITY MANAGEMENT (TFM) FUNCTION	26
4.8	AVAILABILITY	28
4.9	SECURITY MARKINGS AND LABELS FUNCTION	28
4.10	SENSITIVITY LABELS, MARKINGS FUNCTION	29
4.11	TRUSTED USER LOGIN	30
4.12	PUBLIC KEY INFRASTRUCTURE FUNCTIONS	30
4.13	DAC CHECKER FUNCTION	31
4.14	USER ACCESS FUNCTION	33
4.15	LOGIN FUNCTION	33
4.16	SYSTEM ACCESS (LOGIN) AUTHENTICATION FUNCTION	34
4.17	PASSWORD OPERATION FUNCTION	35
4.18	DATA SECURITY FUNCTION	36
4.19	OBJECT REUSE FUNCTION	36
4.20	DATA CONFIDENTIALITY	37
5.0	ACCOUNT MANAGEMENT	37
5.1	ACCOUNT CREATION FUNCTION	37
5.2	ACCOUNT MANAGEMENT FUNCTION	39
6.0	TESTING	40
6.1	FOR DCID 6/3 CERTIFICATION TESTING SHALL BE CONDUCTED INCLUDING VERIFICATION THAT THE FEATURES AND ASSURANCES REQUIRED FOR THE PROTECTION LEVEL ARE FUNCTIONAL	40
6.2	A TEST PLAN AND PROCEDURES SHALL BE DEVELOPED AND INCLUDE:	40

Documentation

ADMSRS= DIICOE Administrative Security Requirements Specification
NMSRS = DIICOE Network Management System Requirements Specification
DCOITM = DCOI Security Requirements Traceability Matrix
DCID = Director of Central Intelligence Directive 6/3
CSE = CSE Directed requirement

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.0 System Functions						
1.1 Console Window Function						
1.1.1 This function shall provide a read-only console window that shall remain open for the life of the user's login session and cannot be closed, although it may be iconified.	X				CSE	
1.1.2 AFDI shall provide a standard set of security support tools to determine the security posture of AFDI systems.	X				DCOIT M	3.2.16.5
1.2 System Support Function						
1.2.1 AFDI shall support both a Solaris and NT operating environment , depending on the platform, which may include: Common Desktop Environment (CDE), X-Windows, Network Interaction, NIS, NIS+, NTP, DNS. Each platform may address these environment variables by different means, however the implementation of the function must uniformly work across platforms.	X				CSE	
1.3 Web Interface Function						
1.3.1 AFDI shall provide a Web interface for infrastructure services.			X		CSE	
1.3.2 AFDI shall provide the capability to detect when the AFDI baseline (kernel, patches and/or segments) has been modified.			X		ADMS RS	3.2.1.71
1.4 Windowing Environment Function						
This function shall:						
1.4.1 Provide a modified version of the XDM, distributed with the MIT X Consortium X11R6.1, to authenticate users.	S				CSE	
1.4.2 Use NT native explorer desktop	N T				CSE	
1.4.3 Provide a screen blanking capability. The time that the workstation may remain idle before the screen is blanked shall be configurable and default to 5 minutes. Either mouse or keyboard input may be used to restore a blank screen. If keyboard input is used, the key used to restore the blank screen shall be ignored.	X				CSE	
1.4.4 Use of screen blanking utilities shall not be permitted except as a feature of AFDI. Software or procedures shall be developed which verify that alternative screen blanking capabilities are not in use.	X				CSE	
1.4.5 Audit login successes and failures at the local workstation. The audit information shall include the user name, platform and time of the event, at a minimum.	X				CSE	
1.4.6 Prohibit logins as the root user at the local workstation.					CSE	
1.4.7 Prohibit logins as the default Administration user at the local workstation	X				CSE	
1.4.8 Provide a multiple login failure capability. If the number of multiple login failures reaches a configurable threshold (3 through 5), the individual is locked out of the workstation where the multiple login failure occurred. Upon lockout, the individual is also prohibited from remotely logging in to the workstation using the vendor-supplied rsh, rlogin, ftp and telnet facilities. If the number of multiple login failures is set to 0, this capability is disabled.	X				CSE	

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.4.8.1 If the number of multiple login failures is set to 0, login capability for the user is disabled.	X				CSE	
1.4.9 Display a security warning prior to the login process which indicates that the system is a classified system and that misuse is subject to the applicable penalties.	X				CSE	
1.4.10 Control the values of the defined environment variables by initializing them to the correct value during the login process.	X				CSE	
1.4.11 Immediately place a user in the windowing environment following a successful login. The windowing environment shall not label the screen with the system's accredited range of operation.	X				CSE	
1.4.12 Immediately terminate the windowing session and display the login screen when a user logs out.	X				CSE	
1.5 Screen Lock Function						
1.5.1 AFDI shall provide a screen-lock capability that is activated if user input devices have been idle for longer than a designated number of minutes which is configurable by a trusted user (e.g., system administrator). The time period shall default to 15 minutes.	X				CSE	
1.5.2 When the screen-lock action is activated, AFDI shall screen-lock the terminal and display a selected screensaver. [not clear that a screensaver should be required as part of the overall AFDI experience. Perhaps better is to specify a "visibly idle display".]	X				CSE	
1.5.3 AFDI shall provide the capability for a trusted user (e.g., system administrator) to disable the screen-lock capability for user(s), group(s), domain(s), or entire system.	X				CSE	
1.5.4 Any user-input device shall be used to initiate actions to restore a screen-locked terminal.	X				DCOIT M	3.2.5.16 .5
1.5.5 The specific input value (whether from keyboard, mouse, or other input device) used to restore a screen-locked terminal shall be ignored except to initiate actions to unlock the terminal.	X				DCOIT M	3.2.5.16 .6
1.5.6 AFDI shall require that users re-authenticate themselves to unlock a screen-locked terminal.	X				DCOIT M	3.2.5.16 .7
1.5.7 The screen-lock capability shall be available for users to activate via icon, menu selection, or button.	X				DCOIT M	3.2.5.16 .8
1.5.8 AFDI shall provide the capability for a trusted user (e.g., system administrator) to unlock a screen-locked terminal irrespective of which user was logged in to that terminal.		X			DCOIT M	3.2.5.16 .9
1.5.9 Screen lock is not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).	X				DCID 6/3	
1.6 Deadman Function This function shall:						

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.6.1 Provide a deadman function that locks the user's terminal if the keyboard and mouse have been idle for longer than a configurable time, defaulting to 5 minutes designated interval, which is configurable by a trusted user (e.g., system administrator) . Either mouse or keyboard input may be used to restore a locked terminal. If keyboard input is used, the key used to restore the locked terminal shall be ignored.	X				CSE	
1.6.2 Modify the xlock mechanism to include auditing and the deadman capability.	X				CSE	
1.6.3 AFDI shall provide the capability for a trusted user (e.g., system administrator) to disable the dead-man capability within the following range:	X				DCOIT M	3.2.5.12 .3
1.6.3.1 Per user(s)			?		DCOIT M	3.2.5.12 .3.1
1.6.3.2 Per Workstation(s)	X				DCOIT M	3.2.5.12 .3.2
1.6.3.3 Per groups(s)			?		DCOIT M	3.2.5.12 .3.3
1.6.3.4 Per administrative domain(s)			?		DCOIT M	3.2.5.12 .3.4
1.6.3.5 Per entire system			?		DCOIT M	3.2.5.12 .3.5
1.6.4 AFDI shall provide a mechanism that generates a notification to a selected trusted user(s) when the dead-man capability activates.	X				DCOIT M	3.2.5.12 .5
1.7 Desktop Manager Function						
This function shall:						
1.7.1 AFDI shall Utilize the windowing manager as specified by DII-COE	X				CSE	
1.7.2 Provide the capability to automatically invoke a desktop manager as part of each user's login process.	X				CSE	
1.7.3 Restrict general users from accessing the operating system shell through configuration of the desktop manager.	X				CSE	
1.8 Database Access and Functionality						
1.8.1 AFDI Security Service functions must operate with the following software:						
1.8.1.1 Relational Data Base Management Systems (RDBMSs):						
1.8.1.1.1 Sybase			X		NMSRS	
1.8.1.1.2 Oracle			X		NMSRS	
1.8.1.1.3 Informix			X		NMSRS	
1.8.2 AFDI DBMSs shall provide the capability to audit user access to databases for the following security relevant events: Attempts to change access control permissions, Attempts to create, copy, sanitize, purge, or execute databases			X		DCOIT M	3.2.18.1
1.8.3 AFDI shall provide the capability to interface with AFDI DBMS(s) to create, modify, and delete database access control permissions (e.g., grant permissions) at the following levels: Table, View, Row or record, Field or element.			X		DCOIT M	3.2.18.2
1.8.4 AFDI shall provide the capability to interface with AFDI DBMS(s) to define access control permissions for the following: User(s), Profile, Workstation.			X		DCOIT M	3.2.18.3

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.8.5 AFDI DBMS(s) shall provide the capability to label (security) database information at the following levels of abstraction: Database, Data row or record			X			3.2.18.5
1.8.6 Security services functions must operate in a distributed computing environment and/or client server environment.			X		ADMS RS	3.3.11
1.9 Functional Timing Requirements						
AFDI shall not prevent the achievement of the following timing requirements:						
1.9.1 AFDI shall provide the capability for a single user login, via the GUI-based login mechanism, (user id and password) to be authenticated in the AFDI within ten (10) seconds. This requirement assumes a properly functioning and configured network.	X				ADMS RS	3.2.3.6
1.9.2 AFDI shall provide the capability for a single user to change profile(s) (via the GUI-based profile change mechanism) and be presented with the appropriate session icons (via the common desktop environment) in the AFDI within twenty (20) seconds. This requirement assumes a properly functioning and configured network.	X				ADMS RS	3.2.3.7
1.9.3 AFDI shall provide the capability for a single user to launch a profile-based application (via the common desktop environment) and be presented with the application in the AFDI within five (5) seconds. This requirement assumes a properly functioning and configured network.	X				ADMS RS	3.2.3.9
1.9.4 AFDI shall provide the capability for a single user to logout of their user session (via the GUI-based logout mechanism) in the AFDI within ten (10) seconds. This requirement assumes a properly functioning and configured network.	X				ADMS RS	3.2.3.10
1.9.5 AFDI shall provide the capability for an administrator to create a single user in the AFDI within four (4) minutes. Creating a user includes defining the following parameters in the appropriate files and databases in the AFDI:	X				ADMS RS	3.2.3.11
1.9.5.1 Unique user identifier	X				ADMS RS	3.2.3.11
1.9.5.2 Login name	X				ADMS RS	3.2.3.11
1.9.5.3 Initial password	X				ADMS RS	3.2.3.11
1.9.5.4 Home directory file server	X				ADMS RS	3.2.3.11
1.9.5.5 Group memberships	X				ADMS RS	3.2.3.11
1.9.5.6 Mail alias(es)	X				ADMS RS	3.2.3.11
1.9.5.7 Shell	X				ADMS RS	3.2.3.11
1.9.5.8 Other user information, e.g., user's real name, telephone	X				ADMS RS	3.2.3.11
1.9.5.9 Profiles	X				ADMS RS	3.2.3.11

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.9.5.10 Other parameters as required by the AFDI as its segments (e.g., DBMS registry)	X				ADMS RS	3.2.3.11
1.9.6 AFDI shall provide the capability for an administrator to create a single profile in the AFDI within two (2) minutes. Creating a profile includes defining the following parameters in the appropriate files and databases in the AFDI:	X				ADMS RS	3.2.3.12
1.9.6.1 Unique profile name	X				ADMS RS	3.2.3.12
1.9.6.2 Account Group	X				ADMS RS	3.2.3.12
1.9.6.3 System Function(s)	X				ADMS RS	3.2.3.12
1.9.6.4 Other parameters as required by the AFDI and its segments (e.g., DBMS permissions (text removed))	X				ADMS RS	3.2.3.12
1.10 Availability					DCOITM	3.2.4
1.10.1AFDI shall be capable of detecting the failure of a system service or resource.	X				DCOIT M	3.2.4.1
1.10.2Audit daemon check	X					
1.10.3AFDI shall provide the capability to generate a notification to a trusted user upon failure of a AFDI system service.	X				DCOIT M	3.2.4.1. 1
1.10.4AFDI shall provide the capability to configure which trusted user(s) shall receive notifications when a system service or resource fails.		X			DCOIT M	3.2.4.1. 1.1
1.10.5The default trusted user who receives notifications when a system service or resource fails shall be the system administrator.		X			DCOIT M	3.2.4.1. 1.1
1.10.6AFDI shall provide the capability to notify a trusted user via Electronic mail message to a trusted user account		X			DCOIT M	3.2.4.1. 2
1.10.7AFDI shall provide the capability to notify a trusted user via a message to the console of a system where the trusted user is logged in		X			DCOIT M	3.2.4.1. 2
1.10.8Failure of a AFDI system service shall be logged in a log file.	X				DCOIT M	3.2.4.1. 3
1.10.9The type of failure and the time of the failure shall be logged.	X				DCOIT M	3.2.4.1. 3
1.10.10 Upon detection of a failed system service, AFDI shall provide the capability to restart the service to a secure state.		X			DCOIT M	3.2.4.1. 4
1.10.11 AFDI shall provide a trusted user the capability to configure how the trusted user is notified when a system service or resource has failed.		X			DCOIT M	3.2.4.1. 5
1.10.12 The primary default capability for notifying the trusted user that a system service or resource has failed is a message to the console of a system where the trusted user is logged in.				X	DCOIT M	3.2.4.1. 5.1
1.10.13 The secondary default capability for notifying the trusted user that a system service or resource has failed is an electronic mail message to a trusted user account.		X			DCOIT M	3.2.4.1. 5.2
1.10.14 Upon recovery of a failed system resource, AFDI shall verify that it returns in a secure state.	X				DCOIT M	3.2.4.2
1.10.15 Upon recovery of a failed system resource, AFDI shall provide the capability to determine if file systems are intact.	X				DCOIT M	3.2.4.2. 1

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
1.10.16 Upon recovery of a failed system resource, AFDI shall provide the capability to determine if access control permissions are unchanged from the state prior to the failure.	X				DCOIT M	3.2.4.2. 2
1.10.17 Upon recovery of a failed system resource, AFDI shall ensure that user privileges have not increased.	X				DCOIT M	3.2.4.2. 3
2.0 User Functions and Utilities						
2.1 Password Tool Function						
2.1.1 Users must authenticate their use of their unique identity code by using a password known to the system before beginning to perform any actions that the system is expected to mediate. Identifications are defined by a trusted user and assigned to the user.	X				CSE	
2.1.2 This function shall provide general users with the ability to change their own passwords and trusted users with the ability to change or expire any general user's password.	X				CSE	
2.1.3 This function does not allow root's password to be changed unless the current password is provided.	X				CSE	
2.1.4 This function Identifies the user who changed the password.	X				CSE	
2.1.5 This function contains password construction rules that are configurable by a trusted user.	X				CSE	
2.2 Changing Password Function						
2.2.1 The password is initially set by a trusted user for a specific user either in creating a new user ID or to recover from a lost password. Subsequently, the user is required to change the password during the first session with the new password. Passwords are required to be changed within a designated time interval regularly thereafter. The password may not be changed sooner than another designated time interval.		X				
2.3 Printed Output Function						
This function shall:						
2.3.1 Utilize the vendor-supplied printing utility, in it's original file system location, to perform the print spooling function.	X				ADMS RS	3.2.1.40
2.3.2 Provide a print function that operates in either a Graphical User Interface (GUI) or command line mode and is invoked whenever any software attempts to invoke utilities directly. The GUI mode shall be the default mode of operation.	X				CSE	
2.3.3 Integrate the print function with the AFDI windowing environment.	X				CSE	
2.3.4 Provide the ability to select the destination printer, number of copies, sensitivity label and handling caveats from a set of authorized values per workstation/server when operating in GUI mode.	X				CSE	
2.3.5 Provide a default listing of the contents of the user's home directory when selecting files to print operating in GUI mode.	X				CSE	
2.3.6 Obtain print options from defaults and command line options. The default value for the hardcopy sensitivity label and handling caveats shall be the system high label of the system.	X				DCOIT M	3.2.8.3

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
2.3.7 Provide print options to set the sensitivity label, handling caveats, command line mode operation, number of copies and destination printer, respectively.	X				CSE	
2.3.8 Surround printed output with banner pages containing the system high label of the system.	X				DCOIT M	3.2.8.3
2.3.9 Label each internal page of printed output at the top and bottom with a sensitivity label and handling caveats.	X				DCOIT M	3.2.8.4. 3
2.3.10 Provide print options to override the printing of the banner pages and internal page labels. The internal page labels shall default to the system high label of the system.	X				DCOIT M	3.2.8.5
2.3.11 Provide for standard printing functions.	X				CSE	
2.4 Secure Email Function						
AFDI shall provide a secure e-mail capability for selected users to:						
2.4.1 Share sensitive information.				X	DCOIT M	3.2.21.1
2.4.2 Encrypt sensitive e-mail traffic.				X	DCOIT M	3.2.21.2
2.4.3 Digitally sign their e-mail transactions.				X	DCOIT M	3.2.21.3
2.4.4 Authenticate the sender of e-mail traffic.				X	DCOIT M	3.2.21.4
2.4.5 Manage public keys for use with e-mail.				X	DCOIT M	3.2.21.5
2.4.6 Manage private keys for use with e-mail.				X	DCOIT M	3.2.21.6
2.4.7 Include attachments to their e-mail traffic.				X	DCOIT M	3.2.21.7
2.4.8 Encrypt attachments in e-mail traffic.				X	DCOIT M	3.2.21.8
2.4.9 Digitally sign attachments in e-mail traffic.				X	DCOIT M	3.2.21.9
2.4.10 Send secure e-mail to multiple recipients.				X	DCOIT M	3.2.21.1 0
2.4.11 Overwrite e-mail messages marked for deletion.				X	DCOIT M	3.2.21.1 1
2.4.12 Validate the integrity of e-mail received.				X	DCOIT M	3.2.21.1 2
2.4.13 Share sensitive information				X	DCOIT M	3.2.21.1 3
2.5 Ping Function						
2.5.1 This function shall provide a GUI for general and privileged users which allows them to determine whether remote workstations/servers are accessible.	X				NMSRS , CSE	3.3.2.3. 9
2.6 Print Status Function						
This function shall:						
2.6.1 Allow a printer's print queue to be monitored.	X				ADMS RS	3.2.1.40
2.6.2 Provide general users with the ability to cancel print requests they have submitted.	X				ADMS RS	3.2.1.40

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
2.6.3 Provide privileged users with the ability to cancel any user's print request.	X				ADMS RS	CSE
2.6.4 Integrate the print status utility with AFDI so that it can be invoked from the workstation's main menu or a desktop manager, if available.	X				ADMS RS	CSE
2.7 User Credentials Function						
This function shall provide the ability to:						
2.7.1 Display users with credentials.	X				CSE	
2.7.2 Display users without credentials.	X				CSE	
2.7.3 Add credentials to users.	X				CSE	
2.7.4 Delete credentials from users.	X				CSE	
2.7.5 Modify a user's credentials.	X				CSE	
3.0 System Administration						
3.1 Printing						
3.1.1 AFDI shall provide the capability to centrally monitor and control print queues in a heterogeneous environment and perform the following administration tasks:	X				ADMS RS	3.2.1.40
3.1.1.1 Display the print queue.	X				ADMS RS	3.2.1.40
3.1.1.2 Start the print queue.	X				ADMS RS	3.2.1.40
3.1.1.3 Stop the print queue.	X				ADMS RS	3.2.1.40
3.1.1.4 Delete print jobs from the print queue.	X				ADMS RS	3.2.1.40
3.1.1.5 Prioritize print jobs in the print queue.				X	ADMS RS	3.2.1.40
3.1.1.6 Move print jobs between print queues.				X	ADMS RS	3.2.1.40
3.1.2 AFDI shall provide the capability to centrally monitor and control printers in a heterogeneous environment and perform the following administration tasks:	X				ADMS RS	3.2.1.41
3.1.2.1 Start printers	X				ADMS RS	3.2.1.41
3.1.2.2 Stop printers	X				ADMS RS	3.2.1.41
3.1.2.3 Flush printers.	X				ADMS RS	3.2.1.41
3.1.3 AFDI shall provide the capability to centrally create print queues in a heterogeneous environment within the administrative domain.	X				ADMS RS	3.2.1.42
3.1.4 AFDI shall provide the capability to centrally delete print queues in a heterogeneous environment within the administrative domain.	X				ADMS RS	3.2.1.43
3.1.5 AFDI shall provide the capability to create printer definitions for the printing systems (whether attached, locally, remote or network), within the administrative domain with the capability to define the following parameters:	X				ADMS RS	3.2.1.44

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.1.5.1 Printer Name(s)	X				ADMS RS	3.2.1.44
3.1.5.2 Printer Type	X				ADMS RS	3.2.1.44
3.1.5.3 Printer Server	X				ADMS RS	3.2.1.44
3.1.5.4 Printer Parameters (e.g., default, flow control)	X				ADMS RS	3.2.1.44
3.1.5.5 Network Printers	X				ADMS RS	3.2.1.44
3.1.5.6 Attached (local or remote) Printers	X				ADMS RS	3.2.1.44
3.1.6 AFDI shall provide the capability to modify printer definitions in the printing system within the administrative domain with the capability to define the following parameters:	X				ADMS RS	3.2.1.45
3.1.6.1 Printer Name(s)	X				ADMS RS	3.2.1.45
3.1.6.2 Printer Type	X				ADMS RS	3.2.1.45
3.1.6.3 Printer Server	X				ADMS RS	3.2.1.45
3.1.6.4 Printer Parameters (e.g., default, flow control)	X				ADMS RS	3.2.1.45
3.1.7 AFDI shall provide the capability to delete printer definitions from the printing system within the administrative domain. The printer deletion mechanism shall provide the capability to reverse all actions associated with printer definition.	X				ADMS RS	3.2.1.46
3.1.8 AFDI shall provide the capability to automatically distribute or make available via network information services printer information to a single host, a group of hosts or all hosts within the administrative domain.	X				ADMS RS	3.2.1.47
3.2 Permissions Function						
3.2.1 AFDI shall provide the capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources (e.g., files, directories and applications), and to assign those privileges to specific users.	X				ADMS RS	3.2.3.4. 1
3.2.2 AFDI shall provide the capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources (e.g., files, directories and applications), and to assign those privileges to specific groups.	X				ADMS RS	3.2.3.4. 2
3.2.3 AFDI shall provide the capability to set the ownership of system resources (e.g., files, directories and applications).	X				ADMS RS	3.2.3.4. 3
3.3 Processes Function						
AFDI shall provide the capability for centralized monitor and control of processes in a heterogeneous environment and perform the following administrative tasks by providing the capability to:						
3.3.1 Display the status of processing resources.	X				ADMS RS	3.2.1.48
3.3.2 Identify active and failed processes.	X				ADMS RS	3.2.1.48

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.3.3 Terminate processes.	X				ADMS RS	3.2.1.48
3.3.4 Suspend processes.	X				ADMS RS	3.2.1.48
3.3.5 Resume processes.	X				ADMS RS	3.2.1.48
3.3.6 Send administrator-defined signals to processes, e.g., SIGHUP.	X				ADMS RS	3.2.1.48
3.4 Network Statistics Function						
3.4.1 This function shall provide the ability to monitor an active network.	X				ADMS RS	3.2.3
3.5 Tools Function						
3.5.1 This function shall provide the ability to execute site pre- configured shell commands.	X				CSE	
3.6 Shell Function						
3.6.1 This function shall provide the ability to access a UNIX shell.	X				CSE	
3.7 Host Credentials Function						
This function provide the ability to:						
3.7.1 Display hosts with credentials.	X				CSE	
3.7.2 Display hosts without credentials.	X				CSE	
3.7.3 Add credentials to hosts.	X				CSE	
3.7.4 Delete credentials from hosts.	X				CSE	
3.7.5 Modify a host's credential.	X				CSE	
3.8 Disk Space Function						
3.8.1 AFDI shall provide the ability to monitor the amount of disk space used by directories and files on a local or remote workstation.	X					
3.8.2 AFDI shall provide the ability to monitor the amount of free disk space on a local or remote workstation.	X					
3.8.3 AFDI shall check the availability of space on each of its disks at regular intervals. If the used space on a disk exceeds a default limit of 85%, or other limit as set by a trusted user, an audit event shall be triggered. In the event of a trigger a notification shall be generated to the designated users, and a predetermined system action shall be performed. System actions may be one or more of the following:				X		
3.8.3.1 System shut down				X		
3.8.3.2 Abort current space demanding tasks				X		
3.8.3.3 Archive and purge inactive files				X		
3.8.3.4 Perform compression on inactive files				X		
3.8.4 AFDI shall provide the capability to control disk resources and perform the following administration tasks:			X		ADMS RS	3.2.1.49
3.8.4.1 Allocate user disk space including setting quotas.			X		ADMS RS	3.2.1.49
3.8.4.2 Modify disk partitions.			X		ADMS RS	3.2.1.49
3.8.4.3 Mount file systems.			X		ADMS RS	3.2.1.49

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.8.4.4 Unmount file systems.			X		ADMS RS	3.2.1.49
3.8.4.5 Determine disk space usage.			X		ADMS RS	3.2.1.49
3.8.4.6 Determine disk space availability.			X		ADMS RS	3.2.1.49
3.8.4.7 Create file systems.			X		ADMS RS	3.2.1.49
3.8.4.8 Modify file systems.			X		ADMS RS	3.2.1.49
3.8.4.9 Create file system tables.			X		ADMS RS	3.2.1.49
3.8.4.10 Modify file system tables.			X		ADMS RS	3.2.1.49
3.8.4.11 Export file system tables.			X		ADMS RS	3.2.1.49
3.8.5 AFDI shall provide the capability to generate a notification if system shutdown is required in order to perform a system diagnostic operation or other system administration function.	X				ADMS RS	3.2.2.21
3.8.6 AFDI shall provide the capability to repair disk blocks.	X				ADMS RS	3.2.2.22
3.9 Performance Management Function						
3.9.1 AFDI shall provide the capability to retrieve usage-related attributes from managed objects. This shall include, as a minimum, the following attributes:	X				ADMS RS	3.2.3.1
3.9.1.1 Processor load in terms of percent of maximum capability	X				ADMS RS	3.2.3.1
3.9.1.2 Disk use in terms of percent of maximum capacity	X				ADMS RS	3.2.3.1
3.9.1.3 Memory use in terms of percent of maximum capacity	X				ADMS RS	3.2.3.1
3.9.2 AFDI shall provide the capability to rename, move, copy and destructively delete files and directories within the administrative domain.	X				ADMS RS	3.2.3.1
3.9.3 AFDI shall provide the capability to initiate an orderly shutdown and generate a notification when a primary power failure is detected within the administrative domain.	X				ADMS RS	3.2.3.23
3.9.4 AFDI shall provide the capability to generate a notification and a log entry when CPU utilization exceeds a specified threshold for a specified period of time.				X	ADMS RS	3.2.3.24
3.10 Host Maintenance Function						
This function shall provide the ability to:						
3.10.1 Maintain a list of host information including hostnames, IP addresses, hostname aliases, ethers and netmasks.	X				CSE	
3.10.2 Maintain the Domain Name Service (DNS) database.	X				CSE	
3.10.3 Implement access to host information via NIS, NIS+, or local files.	S				CSE	
3.10.4 Add, modify, and remove hostnames, IP addresses, hostname aliases, ethers and netmasks.	X				CSE	

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.11 Protocol Maintenance Function						
This function shall provide the ability to:						
3.11.1 Maintain a set of protocols associated with maintained hosts.	X				CSE	
3.11.2 Assign protocols to hosts.	X				CSE	
3.11.3 Specify default protocols automatically added to hosts.	X				CSE	
3.11.4 Display a list of hosts providing a specific protocol. As a site configuration option, users may enter a host that does not appear in the list.	X				CSE	
3.12 Protocol Lister						
3.12.1 Provide a managed list of hosts for applications which access remote hosts (i.e. telnet, FTP, ping, etc).	X				CSE	
3.13 Network Services Function						
3.13.1 AFDI shall provide the capability to configure the LAN ports selection on the workstation within the administrative domain.	X				ADMS RS	3.2.1.67
3.13.2 AFDI shall provide the capability to manually configure the workstation name and IP address within the administrative domain.	X				ADMS RS	3.2.1.68
3.13.3 AFDI shall provide an API or equivalent mechanism that returns a list of logged in users, the user's active and inactive profiles and the user's login host name information.	X				ADMS RS	3.2.1.69
3.13.4 AFDI shall provide the capability to display a list of logged in users	X				ADMS RS	3.2.1.70
3.13.5 AFDI shall provide the capability to display user's active profiles				X		
3.13.6 AFDI shall provide the capability to display inactive profiles				X		
3.13.7 AFDI shall provide the capability to display user's login host name information	X				ADMS RS	3.2.1.70
3.13.8 AFDI shall provide the capability to display update the display when requested by the operator.	X				ADMS RS	3.2.1.70
3.13.9 AFDI shall provide the capability to display assigned sessions	X					
3.13.10 AFDI shall provide the capability to display sessions in use	X					
3.14 Remote Distribution (rdist) Function						
3.14.1 This function shall provide the capability to manage and distribute files from a central location on the network using a GUI provided by AFDI .	S				CSE	
3.14.2 AFDI shall provide the capability for centralized distribution of files and file packages (including directories of files) from a central location to a single host, a group of hosts or all hosts within the administrative domain.	S				CSE	
3.15 Network Time Protocol (NTP) Function						
3.15.1 This function shall provide the ability to synchronize the system clocks of each workstation on the LAN using the NTP.	X				CSE	
3.15.2 AFDI shall provide the capability to specify a drift threshold for time synchronization across the administrative domain.	X				CSE	

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.15.3AFDI shall provide the capability to specify a synchronization method (e.g., abrupt, increase rate) for time synchronization across the administrative domain.	X				CSE	
3.16 Domain Name Service (DNS) Function AFDI shall provide the capability to:						
3.16.1Configure the workstation so that hostnames and IP addresses can be resolved via DNS.	X				CSE	
3.16.2Provide a utility that maintains hostnames in standard format to DNS format.	X				CSE	
3.17 Printer Database Function This function shall:						
3.17.1Provide a GUI based utility for centrally managing a site-wide printer database.	X				CSE	
3.17.2Support the concept of print zones, which are defined to be a group of printers to which a workstation is authorized to submit print requests.	X				CSE	
3.17.3Generate and distribute individual workstation/server printer databases in the native format of the platform on the basis of its print zone, such that only those printers in the same zone as the workstation/server are defined.	X				CSE	
3.18 Host Services Function AFDI shall provide the capability for centralized host definition in a heterogeneous environment with the capability to define the following host parameters:						
3.18.1Hostname	X				ADMS RS	3.2.1.31
3.18.2IP Address	X				ADMS RS	3.2.1.31
3.18.3Hostname aliases	X				ADMS RS	3.2.1.31
3.18.4AFDI shall provide the capability to automatically distribute or make available via network information services, host information to a single host, a group of hosts or all hosts within the administrative domain.	X				ADMS RS	3.2.1.32
3.19 Peripherals Function AFDI shall provide the capability to monitor and control peripherals within the administrative domain such as:						
3.19.1CDROMS			X		ADMS RS	3.2.1.52
3.19.2Printers	X				ADMS RS	3.2.1.52
3.19.3Tape drives			X		ADMS RS	3.2.1.52
3.19.4AFDI shall provide the capability to allocate access to peripherals.			X		ADMS RS	3.2.1.52 a
3.19.5AFDI shall provide the capability for centralized reboot and shutdown of a single host, a group of hosts or all hosts within the administrative domain.	X				ADMS RS	3.2.1.53
3.20 Sessions Function This function shall provide the ability to:						

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.20.1 Ensure a definable sets of applications are associated with a login session.	X				CSE	
3.20.2 Define, change and delete work environments. Work environments provide a means to associate definable sets of applications with a login session. [It must be possible to define, change and delete such sets of applications]	X				CSE	
3.20.3 Set application specific environment variables prior to invoking the application. [It must be possible to set values needed by applications prior to their invocation. These include environment variables, command-line parameters etc.]	X				CSE	
3.20.4 Control the general user's environment (e.g. by controlling the contents of files such as those listed below: ~/username/.Xdefaults ~/username/.login ~/username/.motifbind ~/username/.mwmrc ~/username/.xinitrc ~/username/.profile ~/username/.xsession ~/username/.cshrc)	X				CSE	
3.20.5 Control the work environments available to each general user.	X				CSE	
3.21 Account Maintenance Function						
This function shall provide the ability to:						
3.21.1 Add and remove groups.	X				CSE	
3.21.2 Assign general users a trusted role.	X				CSE	
3.21.3 Add and remove general users.	X				CSE	
3.21.4 Modify general user account information.	X				CSE	
3.21.5 Enable and disable general user accounts.	X				CSE	
3.21.6 Support automounted user home directories.	X				CSE	
3.22 Account Information Function						
This function shall provide the ability to:						
3.22.1 Determine general users currently logged on.	X				CSE	
3.22.2 Determine valid general users.	X				CSE	
3.22.3 Clear locked user accounts on either local or remote workstations.	X				CSE	
3.23 Reboot Function						
3.23.1 This function shall provide the ability to shutdown or reboot multiple local or remote workstations from a local disk or network server. When invoked, the function shall generate an audit indicating when each workstation was shutdown or rebooted.	X					
3.24 Alert Function						
3.24.1 This function shall provide the ability to generate an alert message and display it on each workstation with logged in users.	X					
3.25 Process Management Function						
3.25.1 This function shall provide the ability to manage local and remote process tables.	X					
3.26 Alert Messages Function						
The following conditions shall cause an alert to be transmitted to selected users:						
3.26.1 Detection of malicious code on hard drives or removable media				X		
3.26.2 Detection of malicious code in incoming data streams				X		

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.26.3Data storage nearing critical capacity on a hard drive or removable medium				X		
3.26.4A user ID is locked				X		
3.26.5Dead man capability activates				X		
3.26.6Audit data has reached the current limit of available storage capacity				X	DCOIT M	3.2.2.15
3.26.7Audit process(s) has failed				X	DCOIT M	3.2.3.1. 4
3.26.8Failure of a AFDI system service				X	DCOIT M	3.2.4.1. 1
3.26.9Time to perform audit archive ??				X	DCOIT M	3.2.3.1. 5.4
3.26.10 Alerts shall take the form of:						
3.26.10.1Visible message on the workstation screen				X	DCOIT M	3.2.13.4 .3.1
3.26.10.2Audible alarm				X	DCOIT M	3.2.13.4 .3.2
3.27 Segmentation Function						
3.27.1AFDI shall provide the capability for Point and Click/Drag and Drop Segmentation			X			
3.27.2AFDI shall provide the capability to perform Configuration Definition Modeling			X			
3.27.3AFDI shall provide the capability for Segment enhancements			X			
3.27.4AFDI shall provide a web based interface for the segmentation process			X			
3.27.5AFDI shall provide the capability for Segment testing			X			
3.28 Installation & Configuration Function						
3.28.1THE AFDI segment shall be installable using the DII COE segment installer and adhere to standard segmentation requirements.	X					
3.28.2A Graphical interface configuration control tool set shall be provided which will allow the installer to specify parameters specific to the workstation, and will allow specification of the specific services to be enabled as client and or server processes.	X					
3.28.3The ability to populate user, group, host, and printer related information shall be provided from existing local, NIS or NIS+ maps.	S					
3.28.4The configuration control tool(s) shall be operable for initial configuration, or for reconfiguration as needs and interfaces change over time.	X					
3.28.5The installation/configuration tool shall be capable of obtaining system configuration information (NTP role, user population, CLASS roles for example) from a data segment. This provides an automated alternative to manually specifying configuration information via the GUI for each workstation	X					
3.28.6Shall provide GUI-interface configuration utilities for support of network management tools (tools used to maintain user account, host name, group and printer databases.)						

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.28.7 Configuration utilities shall be capable of configuring or reconfiguring which operating system information tables/files are to be maintained, (NIS, NIS+, /etc files, NT account manager,) domain name, and which host will be used for the update						
3.28.8 Configuration utilities shall allow specifying or changing default values for new managed entries						
3.28.9 Non-Destructive load and upgrade capability. Configuration utilities shall have the capability to populate managed information tables/files from existing operating system native tables or files, without requiring re-creation of user accounts or host table entries.						
3.29 Automated Installation Function						
Provide support for rapid, efficient installation of multiple workstations resulting in fully configured and functional systems via:						
3.29.1 Operating system network-based installs (Jumpstart or NT Unattended Installs)						
3.29.1.1 Native operating system installation & configuration		X			AFDI	1.0 CCB
3.29.1.2 Patches installation & configuration		X			AFDI	1.0 CCB
3.29.1.3 DII COE Kernel installation & configuration		X			AFDI	1.0 CCB
3.29.1.4 AFDI segment installation & configuration		X			AFDI	1.0 CCB
3.29.1.5 End-user application segment(s) installation & configuration		X			AFDI	1.0 CCB
3.29.2 Per-workstation disk copy/reconfiguration (disk cloning) method						
3.29.2.1 A GUI interface shall be provided for configuration and operation of Disk Cloning.		X			AFDI	1.0 CCB
3.29.2.2 Two basic sets of functions shall be provided, Disk copying, and Disk Reconfiguration.		X			AFDI	1.0 CCB
3.29.2.3 The Disk Copy functionality shall provide for an option of intermediate storage of the disk image.		X			AFDI	1.0 CCB
3.29.2.4 Intermediate storage options shall include to a file, (NFS mounted or local), or to a local workstation tape drive.		X			AFDI	1.0 CCB
3.29.2.5 In the case of intermediate disk image storage, the tape or intermediate storage directory shall contain any files required for a user to be able to build a functioning workstation from either single user mode (from Operating System CD-ROM) or from an alternate boot disk running the target operating system. (tape use example: extract first tar set from tape, followed by restore)		X			AFDI	1.0 CCB
3.29.2.6 Copy shall allow for altering partition sizes.		X			AFDI	1.0 CCB
3.29.2.7 Disk Reconfiguration utility shall be capable of being executed independently from the disk copy function. This will allow stockpiling disk clones for configuration as required, and shall also allow for use of the utility to modify an operational workstation without first copying the disk.		X			AFDI	1.0 CCB

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
3.29.2.8 Disk Reconfiguration shall modify file contents on the disk as required to allow system boot and operation. The following should be changeable at a minimum: Operating SCSI ID, Host Name, IP address.		X			AFDI	1.0 CCB
4.0 Security Management						
4.1 Security Administration Function						
4.1.1 AFDI shall provide the capability to centrally monitor and control system and application log files within the administrative domain and perform the following administration tasks:	X				ADMS RS	3.2.1.54
4.1.1.1 View log files.	X				ADMS RS	3.2.1.54
4.1.1.2 Purge log files.	X				ADMS RS	3.2.1.54
4.1.1.3 Archive log files to a selected storage medium.	X				ADMS RS	3.2.1.54
4.1.1.4 Print log files to a selected printer.	X				ADMS RS	3.2.1.54
4.1.1.5 Compress log files.	X				ADMS RS	3.2.1.54
4.1.1.6 Control the size of the log files.	X				ADMS RS	3.2.1.54
4.1.1.7 Enable/disable logging.	X				ADMS RS	3.2.1.54
4.1.1.8 Search log files.	X				ADMS RS	3.2.1.54
4.1.1.9 Sort log files.				X	ADMS RS	3.2.1.54
4.1.1.10 Query log files.				X	ADMS RS	3.2.1.54
4.1.1.11 Save log files to other files.				X	ADMS RS	3.2.1.54
4.2 Accountability						
4.2.1 AFDI shall provide the GUI-based capability to check whether or not the AFDI components are operating in a secure mode in accordance with the Security Requirements (as defined in the Security Services SRS) and to perform the following administrative tasks:	S	N T			ADMS RS	3.2.4.1. 1
4.2.2 AFDI shall provide the capability to ensure security relevant system files and directories do not have dangerous access permissions (e.g., world writable or world readable).	X				ADMS RS	3.2.4.1. 1
4.2.3 AFDI shall provide the capability to examine the boot commands to ensure that files or paths referenced are not world writable.	X				ADMS RS	3.2.4.1. 1
4.2.4 AFDI shall provide the capability to ensure system devices are not world writable or world readable and that systems have not been shared without any restrictions.	X				ADMS RS	3.2.4.1. 1

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.2.5 AFDI shall provide the capability to analyze the local or network user database and flag accounts with improperly constructed passwords in accordance the Security SRS, improper number of fields, non-unique user identifiers, and blank lines.	X				ADMS RS	3.2.4.1. 1
4.2.6 AFDI shall provide the capability to analyze the local or network group database and flag accounts with improperly constructed passwords in accordance the Security SRS, improper number of fields, non-unique group identifiers, blank lines and groups with duplicative members.	X				ADMS RS	3.2.4.1. 1
4.2.7 AFDI shall provide the capability to analyze trusted access to the system.	X				ADMS RS	
4.2.8 AFDI shall provide the capability to examine user home directories and specific files in each home directory to ensure they are not world writable.	X				ADMS RS	
4.2.9 AFDI shall provide the capability to check for unexpected file system corruption or security breaches using Cyclic Redundancy Checks (CRCs) and changes to a file's inode attributes.	S			N T	ADMS RS	3.2.4.1. 11
4.2.10AFDI shall provide the capability to measure intrusion detection by reporting changes to a file's RSA MD5 encryption signature.				X	ADMS RS	3.2.4.1. 11
4.2.11AFDI shall provide the capability to enable/disable security-relevant audit events within the administrative domain.	X				ADMS RS	3.2.4.1. 1
4.2.12AFDI shall provide the capability for centralized audit reduction in a heterogeneous, distributed environment with the capability to selectively filter the audit records in accordance with the Security Requirements.	X				ADMS RS	3.2.4.1. 4
4.3 Audit Function						
This function shall:						
4.3.1 Provide an auditing function capable of accepting application level audit logging requests.	X					
4.3.2 Provide an audit Application Programming Interface (API) which shall define a standard audit format and shall be used for application level auditing.	X					
4.3.3 Define the system-level audit events that are to be collected.	X					
4.3.4 Be protected from change or deletion by general users.	X				DCOIT M	3.2.3.1. 2
4.3.5 AFDI shall provide the capability for centralized audit trail management with the capability to perform the following administrative tasks:	X				ADMS RS	3.2.4.1. 5
4.3.5.1 View the raw audit trail.	X				ADMS RS	3.2.4.1. 5
4.3.5.2 View the reduced audit trail.	X				ADMS RS	3.2.4.1. 5
4.3.5.3 Backup/archive the audit trail to a selectable device.	X				ADMS RS	3.2.4.1. 5

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.3.5.4 Restore the audit trail from a selectable device.	X				ADMS RS	3.2.4.1. 5
4.3.5.5 Delete the audit trail. The audit deletion capability shall not delete the audit trail without verifying the action with the administrator.	X				ADMS RS	3.2.4.1. 5
4.3.6 AFDI shall provide the capability to assign passwords to users.	X				ADMS RS	3.2.4.1. 6
4.4 Logging and Security Audit Function						
4.4.1 AFDI shall provide the capability to create, maintain, process, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects.	X				DCOIT M	3.2.3.1
4.4.2 AFDI shall protect audit data so that access to it is limited to those who are authorized to view audit data.	X				DCOIT M	3.2.3.1. 1
4.4.3 AFDI shall protect the audit processes and audit data from change or deletion by general users. At a minimum, AFDI shall protect the following:	X				DCOIT M	3.2.3.1. 2
4.4.3.1 Audit mechanisms (e.g., executable files).	X				DCOIT M	3.2.3.1. 2.1
4.4.3.2 Configuration parameters (e.g., audit configuration files).	X				DCOIT M	3.2.3.1. 2.2
4.4.3.3 Capability to enable or disable audit processes.	X				DCOIT M	3.2.3.1. 2.3
4.4.4 Provide a mechanism that generates a notification when the audit data has reached a configurable threshold of n percent of available storage capacity.	X				DCOIT M	3.2.3.1. 3
4.4.5 Be configurable by a trusted user to provide a capability for recovery in the event that the threshold n percent of available storage capacity has been exceeded. At a minimum, the following capabilities shall be provided:	X				DCOIT M	3.2.3.1. 3.1
4.4.5.1 Halt the system	X				DCOIT M	3.2.3.1. 3.1.1
4.4.5.2 Overwrite the oldest audit data	X				DCOIT M	3.2.3.1. 3.1.2
4.4.5.3 Discontinue auditing	X				DCOIT M	3.2.3.1. 3.1.3
4.4.5.4 Increase storage capacity for audit data				X	DCOIT M	3.2.3.1. 3.1.4
4.4.6 Provide an interface for configuring which trusted user shall receive notifications when the audit data has reached the threshold n percent of available storage capacity.				X	DCOIT M	3.2.3.1. 3.1.3.1
4.4.7 May be manual or command line implementable	X				DCOIT M	
4.4.8 Provide the capability for a trusted user to configure the threshold percent of available storage capacity when a notification shall be generated.	X				DCOIT M	3.2.3.1. 3.3
4.4.9 The default threshold shall be 85 percent.	X				DCOIT M	3.2.3.1. 3.3.1
4.4.10 Provide a mechanism that generates a notification to a trusted user when the audit process(s) has failed.		X			DCOIT M	3.2.3.1. 4

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.4.11 Provide a capability for recovery in the event that the audit process(s) has failed. At a minimum, the following capabilities shall be provided:	X				DCOIT M	3.2.3.1. 4.1
4.4.11.1.1 Halt the system		X			DCOIT M	3.2.3.1. 4.1.1
4.4.11.1.2 Suspend user processing until audit process(s) are restarted		X			DCOIT M	3.2.3.1. 4.1.2
4.4.11.1.3 Notify a trusted user of the failure.		X			DCOIT M	3.2.3.1. 4.1.3
4.4.11.1.4 Restart the audit process(s)	X				DCOIT M	3.2.3.1. 4.1.4
4.4.11.1.5 Notify a trusted user of the failure.		X			DCOIT M	3.2.3.1. 4.1.4
4.4.12 The default recovery capability shall be to restart audit process(s) and notify a trusted user of the failure.		X			DCOIT M	3.2.3.1. 4.1.4.1
4.4.13 Provide an interface for configuring which trusted user shall receive notifications when the audit process(s) has failed.		X			DCOIT M	3.2.3.1. 4.2
4.4.14 AFDI shall provide the capability to archive and selectively retrieve audit data				X	DCOIT M	3.2.3.1. 5
4.4.15 AFDI shall provide the capability to automatically archive audit data when the audit data reaches a configurable threshold of percent of available storage capacity.				X	DCOIT M	3.2.3.1. 5.1
4.4.16 AFDI shall provide the capability for a trusted user to configure the threshold of n percent upon which audit data shall be automatically archived.				X	DCOIT M	3.2.3.1. 5.2
4.4.17 The default threshold shall be 70 percent.				X	DCOIT M	3.2.3.1. 5.2.1
4.4.18 AFDI shall provide the capability for a trusted user to configure a timer of day n upon which audit data shall be automatically archived.	X				DCOIT M	3.2.3.1. 5.3
4.4.19 The default time of day n shall be 0000 hours.	X				DCOIT M	3.2.3.1. 5.3.1
4.4.20 Provide a mechanism that generates a time configurable notification to remind a trusted user (e.g., system administrator) to perform audit archive.	X				DCOIT M	3.2.3.1. 5.4
4.4.21 Provide a GUI for a trusted user to configure the time, represented as every n hours.				X	DCOIT M	3.2.3.1. 5.4.1
4.4.22 The default threshold n shall be every 168 hours.				X	DCOIT M	3.2.3.1. 5.4.2
4.4.23 AFDI shall provide the capability to enable and disable auditable events.	X				DCOIT M	3.2.3.2
4.4.24 AFDI shall provide the capability to audit the following types of events	X				DCOIT M	3.2.3.3
4.4.25 Use of identification and authentication mechanisms	X				DCOIT M	3.2.3.3. 1
4.4.26 Introduction of designated objects into a user's address space (e.g., file open, program initiation)	X				DCOIT M	3.2.3.3. 2
4.4.27 Creation, modification, and deletion of designated objects	X				DCOIT M	3.2.3.3. 3

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.4.28 Actions taken by trusted users	X				DCOIT M	3.2.3.3. 4
4.4.29 Production of printed output	X				DCOIT M	3.2.3.3. 5
4.4.30 Override of human-readable output markings	X				DCOIT M	3.2.3.3. 6
4.4.31 Change in access control permissions	X				DCOIT M	3.2.3.3. 7
4.4.32 Export to external media	X				DCOIT M	3.2.3.3. 8
4.4.33 System startup	X				DCOIT M	3.2.3.3. 9
4.4.34 System shutdown	X				DCOIT M	3.2.3.3. 10
4.4.35 Deadman activation	X				DCOIT M	3.2.3.3. 11
4.4.36 Information to collect					DCOIT M	3.2.3.5
4.4.37 AFDI shall provide the capability for a trusted user to define security-relevant events. For each recorded event, at a minimum AFDI audit record shall identify:	X				DCOIT M	3.2.3.5. 1
4.4.37.1 System date and time (to the nearest second) of the event	X				DCOIT M	3.2.3.5. 2
4.4.37.2 User ID	X				DCOIT M	3.2.2.5. 3
4.4.37.3 Type of event	X				DCOIT M	3.2.3.5. 4
4.4.37.4 Success or failure of the event	X				DCOIT M	3.2.3.6
4.4.38 For identification and authentication events, AFDI audit record shall identify the origin of the request (e.g., terminal ID, host IP address).	X				DCOIT M	3.2.3.7
4.4.39 For events that introduce an object into a user's address space, and for object deletion events, AFDI audit record shall identify the name of the object.				X	DCOIT M	3.2.3.7
4.4.40 AFDI Shall provide the capability to selectively audit the actions of any one or more users based on individual identity.	X				DCOIT M	3.2.3.8
4.4.41 Provide the capability to correlate all system administrative and audit logs (e.g., database management system logs, operating system audit logs, and other system logs) within an administrative domain.	X				DCOIT M	3.2.3.9
4.4.42 Provide the capability to receive application-level audit data (e.g., UNIX syslog, Windows NT event log).	X				DCOIT M	3.2.3.10
4.4.43 Provide the capability to generate reports of audit data that has been collected.	X				DCOIT M	3.2.3.11
4.4.44 Provide the capability to generate reports based on fields in event records or Boolean combinations of those fields.				X	DCOIT M	3.2.3.11 .1
4.4.45 Provide the capability to generate reports based on ranges of system date and time that audit records were collected.	X				DCOIT M	3.2.3.11 .2

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.4.46AFDI shall provide the capability for a trusted user to selectively revoke a user's access to services.	X				DCOIT M	3.2.4.3
4.4.47AFDI shall provide the capability for trusted users to generate reports of audit data that has been collected based on fields in event records or Boolean combinations of those fields, or based on ranges of system date and time that audit records were collected.				X	DCOIT M	3.2.3.11
4.5 Security and Confidentiality Requirements						
4.5.1 AFDI shall provide for the management of the network, system and security mechanisms and be comprised of a set of management application entities and a management communications protocol stack.				X	ADMS RS	3.3.7
4.5.2 AFDI capabilities shall be certifiable, initially for the system high mode of operation in a heterogeneous, distributed environment as well as a stand-alone environment.	X				ADMS RS	3.3.7.1
4.5.3 The security administration functions shall be logically separated from other system administration functions, such that only authorized administrative personnel can access them.	X				ADMS RS	3.3.7.2
4.5.4 AFDI security devices shall operate under a common security policy. The security devices may; however, be controlled from different management centers and hence belong to different management domains.	X				ADMS RS	3.3.7.3
4.6 Centralized Log/Audit Support Subsystem (CLASS) Function The CLASS Server component shall:						
4.6.1 Provide a Central Audit Collection Server (CACS) that collects the full range of native audit and log data from either workstations/servers or Intermediate Audit Collection Servers (IACSs).	X				CSE	
4.6.2 Provide a hierarchical configuration of CACSs and IACSs.	X				CSE	
4.6.3 Provide filter mechanisms on the CACS for processing audit and log data prior to storage.	X				CSE	
4.6.4 Run on one or more of the AFDI platforms (specified in 3.2.9).	X				CSE	
4.6.5 Be protected from change or deletion by general users.	X				CSE	
This CLASS client component shall:						
4.6.6 Provide configurable automatic and manual initiation of the transfer of audit and log data from workstations/servers to an IACS or CACS.	X				CSE	
4.6.7 Provide configurable automatic and manual initiation of the upload of audit and log data from an IACS to the CACS.	X				CSE	
4.6.8 Provide filter mechanisms for processing audit and log data prior to transferring the data to a IACS or CACS.	X				CSE	
This CLASS user agent component shall:						
4.6.9 Provide manual initiation of the transfer of audit and log data from workstations/servers to either an IACS or the CACS.	X					CSE
4.6.10Provide manual initiation of the transfer of audit and log data from an IACS to the CACS.	X					CSE
4.6.11Allow the selective review of audit data based on, at a minimum, the identity of individuals and the type of audit event.	X					CSE

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.6.12 Allow audit and log data stored on an IACS or CACS to be archived and deleted.	X					CSE
4.6.13 Provide a single results window for the download or retrieval of files.	X					CSE
4.7 Trusted Facility Management (TFM) Function						
4.7.1 The TFM function shall provide support for separate trusted roles. AFDI shall be delivered with three configurable, sample trusted roles: ISSO, Systems Administrator and Operator.	X				CSE	
4.7.2 The TFM function shall require users, via login, to authenticate themselves prior to accessing a trusted role.	X				CSE	
4.7.3 The TFM function shall allow the privileges available from each trusted role to be shared and dynamically assigned.	X				CSE	
4.7.4 The TFM function shall provide the trusted role interface to populate or change the privileges assigned to a trusted role	X				CSE	
4.7.5 The TFM function shall allow information contained in a privilege's GUI to be quickly located through implementation of a search capability.	X				CSE	
4.7.6 AFDI shall support trusted facility management via segregation of authorized roles.	X				DCOIT M	3.2.16.1
4.7.7 At a minimum AFDI shall provide security officer, system administrator, and user roles.	X				DCOIT M	3.2.16.1 .1
4.7.8 AFDI shall provide the capability for a trusted user (e.g., system administrator) to create trusted role(s).	X				DCOIT M	3.2.16.1 .2
4.7.9 AFDI shall provide the capability for a trusted user (e.g., system administrator) to assign function(s) to a trusted role(s) and/or group(s).	X				DCOIT M	3.2.16.1 .3
4.7.10 AFDI shall provide the capability for a trusted user (e.g., system administrator) to modify trusted role(s).	X				DCOIT M	3.2.16.1 .4
4.7.11 AFDI shall provide the capability for a trusted user (e.g., system administrator) to add function(s) to a trusted role(s) and/or group(s).	X				DCOIT M	3.2.16.1 .4.1
4.7.12 AFDI shall provide the capability for a trusted user (e.g., system administrator) to delete function(s) from a trusted role(s) and/or group(s).	X				DCOIT M	3.2.16.1 .4.2
4.7.13 AFDI shall provide the capability for a trusted user (e.g., system administrator) to modify function(s) from a trusted role(s) and/or group(s).	X				DCOIT M	3.2.16.1 .4.3
4.7.14 AFDI shall prohibit a trusted role from being able to delete or modify transactions performed by that trusted role.	X				DCOIT M	3.2.16.1 .4.4
4.7.15 AFDI shall provide the capability for a trusted user (e.g., system administrator) to delete trusted role(s) and/or group(s).	X				DCOIT M	3.2.16.1 .5
4.7.16 AFDI shall provide the capability for a trusted user (e.g., system administrator) to manage user accounts.	X				DCOIT M	3.2.16.2
4.7.17 AFDI shall provide the capability for a trusted user (e.g., system administrator) to create user accounts.	X				DCOIT M	3.2.16.2 .1
4.7.18 AFDI shall provide the capability for a trusted user (e.g., system administrator) to delete user accounts.	X				DCOIT M	3.2.16.2 .2
4.7.19 AFDI shall provide the capability for a trusted user (e.g., system administrator) to manage profile(s) and/or group(s).	X				DCOIT M	3.2.16.2 .3

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.7.20AFDI shall provide the capability for a trusted user (e.g., system administrator) to create profile(s) and/or group(s).	X				DCOIT M	3.2.16.2 .3.1
4.7.21AFDI shall provide the capability for a trusted user (e.g., system administrator) role to modify the access rights of profile(s) and/or group(s).	X				DCOIT M	3.2.16.2 .3.2
4.7.22AFDI shall provide the capability for a trusted user (e.g., system administrator) to delete profile(s) and/or group(s) of users.	X				DCOIT M	3.2.16.2 .3.3
4.7.23AFDI shall provide the capability for a trusted user (e.g., system administrator, security officer) to lock and unlock user accounts.	X				DCOIT M	3.2.16.2 .4
4.7.24AFDI shall provide the capability to purge data from fixed and removable storage media or assignable storage devices.	X				DCOIT M	3.2.16.4
4.7.25AFDI shall provide a standard set of security support tools to determine the security posture of AFDI systems.	X				DCOIT M	3.2.16.5
4.7.26AFDI shall provide the capability to validate that passwords have met the requirements for password characteristics	X				DCOIT M	3.2.16.5 .1
4.7.27AFDI shall provide the capability to determine if changes have been made to designated systems and applications files, (e.g., password or rc.* files).	X				DCOIT M	3.2.16.5 .2
4.7.28AFDI shall provide the capability for a trusted user to monitor and analyze the configuration of a host.	X				DCOIT M	3.2.16.5 .3
4.7.29AFDI shall provide the capability to verify the configuration of a system to ensure that the security policy has been implemented (i.e., check for current security patches, check that unneeded network services are turned off).	X				DCOIT M	3.2.16.5 .3.1
4.7.30AFDI shall provide the capability for a trusted user to manage sensitivity labels and handling caveats used in marking printed output.	X				DCOIT M	3.2.16.6
4.7.31AFDI shall provide the capability for a trusted user to enable or disable marking printed output with sensitivity labels and handling caveats.	X				DCOIT M	3.2.16.6 .1
4.7.32AFDI shall provide the capability for a trusted user to create a set of authorized sensitivity labels and handling caveat values for use in marking printed output.	X				DCOIT M	3.2.16.6 .2
4.7.33AFDI shall provide the capability for a trusted user to modify the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.	X				DCOIT M	3.2.16.6 .3
4.7.34AFDI shall provide the capability for a trusted user to delete the set of authorized sensitivity label and handling caveat values that are used in marking printed output.	X				DCOIT M	3.2.16.6 .4
4.7.35AFDI shall provide the capability for a trusted user (e.g., security officer) to configure all audit functionality.	X				DCOIT M	3.2.16.7
4.7.36AFDI shall provide the following capabilities for a trusted user (e.g., security officer) for managing the audit log(s):					DCOITM	
4.7.36.1 Selectively view	X				DCOIT M	3.2.16.7 .1.1
4.7.36.2 Selectively print	X				DCOIT M	3.2.16.7 .1.2

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.7.36.3 Archive	X				DCOIT M	3.2.16.7 .1.3
4.7.36.4 Selectively restore	X				DCOIT M	3.2.16.7 .1.4
4.7.36.5 Backup	X				DCOIT M	3.2.16.7 .1.5
4.7.36.6 Selectively delete	X				DCOIT M	3.2.16.7 .1.6
4.7.36.7 Sort				X	DCOIT M	3.2.16.7 .1
4.7.36.8 Reduce	X				DCOIT M	3.2.16.7 .1.8
4.7.37AFDI shall provide the capability to separately assign each of the following audit functions to separate trusted roles (e.g., security officer, system administrator):	X				DCOIT M	3.2.16.7 .2
4.7.37.1 Backup and recover audit data file(s)	X				DCOIT M	3.2.16.7 .2.1
4.7.37.2 Archive audit data file(s)	X				DCOIT M	3.2.16.7 .2.2
4.7.37.3 Delete audit data file(s)	X				DCOIT M	3.2.16.7 .2.3
4.7.37.4 Restore audit data file(s)	X				DCOIT M	3.2.16.7 .2.4
4.7.37.5 Review online audit data file(s).	X				DCOIT M	3.2.16.7 .2.5
4.7.38AFDI shall be configurable to prevent all but a trusted user (e.g., security officer) access to audit log(s) and audit functionality.	X				DCOIT M	3.2.16.8
4.7.39AFDI shall be configurable to prevent all but a trusted user (e.g., system administrator) access to account, profile, and group management functionality.	X				DCOIT M	3.2.16.9
4.7.40AFDI shall provide the capability to assign security, system administration, database administration, and network administration function(s) to multiple trusted roles, allowing levels of responsibility within a trusted role to be created.	X				DCOIT M	3.2.16.1 0
4.7.41AFDI shall provide the capability for a trusted user (e.g., security officer) to restrict access to system resources, objects, files, hardware, etc from user(s) and/or groups.	X				DCOIT M	3.2.16.1 1
4.8 Availability						
4.8.1 AFDI shall support trusted roles as defined in the DII-COE Security Services SRS.	X					
4.8.2 AFDI shall limit the system functions assigned to a trusted role to those required to perform the trusted role effectively as defined in the I&RTS.	X					
4.8.3 AFDI shall prohibit security relevant functions from being assigned to non-trusted roles. Security relevant functions include those functions which may affect the implementation of the security policy within AFDI.	X					
4.9 Security Markings and Labels Function						

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.9.1 AFDI shall provide the capability to view the network names and addresses of all network-addressable managed objects in the management domain. Network-addressable refers to host resources, such as hosts and network printers, that can be assigned network names and network addresses and can be accessed via the enterprise network.	X				ADMS RS	3.2.1.61
4.9.2 AFDI shall provide the capability to assign network names and addresses of all network-addressable host resources (i.e., managed objects) in the management domain.	X				ADMS RS	3.2.1.62
4.9.3 AFDI shall provide the capability to modify network names and addresses of all network-addressable host resources (i.e., managed objects) in the management domain.	X				ADMS RS	3.2.1.63
4.9.4 AFDI shall provide the capability to manage sensitivity labels and handling caveats used in marking printed output with sensitivity labels and handling caveats.	X				ADMS RS	3.2.4.3. 4
4.9.5 AFDI shall provide the capability to enable or disable marking printed output with sensitivity labels and handling caveats.	X				ADMS RS	3.2.4.3. 5
4.9.6 AFDI shall provide the capability for creating a set of authorized sensitivity labels and handling caveat values for use in marking printed output.	X				ADMS RS	3.2.4.3. 6
4.9.7 AFDI shall provide the capability for modifying the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.	X				ADMS RS	3.2.4.3. 7
4.9.8 AFDI shall provide the capability for deleting of the set of authorized sensitivity label and handling caveat values that are used in marking printed output.	X				ADMS RS	3.2.4.3. 8
4.10 Sensitivity Labels, Markings Function						
4.10.1AFDI shall display a security warning prior to the login process that indicates the highest classification of information processed on the system.	X				DCOIT M	3.2.8.1
4.10.2AFDI shall display a security warning during the login process that indicates misuse of the system is subject to applicable penalties.	X				DCOIT M	3.2.8.2
4.10.3This security warning shall state that the user accepts responsibility for his or her actions prior to being permitted to access information.	X				DCOIT M	3.2.8.2. 1
4.10.4AFDI shall provide the capability to surround each print job with banner pages reflecting the system high sensitivity level of the system.	X				DCOIT M	3.2.8.3
4.10.5AFDI shall provide the capability to label the top and bottom or top only or bottom only of each internal page of printed output with a sensitivity label representing the sensitivity of the output.	X				DCOIT M	3.2.8.4
4.10.6The internal page markings shall default to the system high sensitivity level of the system.	X				DCOIT M	3.2.8.4. 1
4.10.7The internal page markings shall default to label at the top and bottom of each page.	X				DCOIT M	3.2.8.4. 3

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.10.8AFDI shall provide an authorized user with print options to override the printing of the banner pages and/or internal page markings.	X				DCOIT M	3.2.8.5
4.10.9AFDI shall provide the capability to audit any override of the printing of banner pages and internal page markings.	X				DCOIT M	3.2.8.5. 1
4.10.10 AFDI shall provide the capability for a trusted user to control which users can override printing of banner pages and internal page markings		X			DCOIT M	3.2.8.5. 2
AFDI shall provide the following forms of markings for labeling printed output:						
4.10.11 Highest classification of information processed on the system	X				DCOIT M	3.2.8.6. 1
4.10.12 Applicable markings (codewords, dissemination and control markings and handling caveats)	X				DCOIT M	3.2.8.6. 3
4.10.13 AFDI shall provide the interface from which an authorized user selects the sensitivity label from the set of authorized markings.	X				DCOIT M	3.2.8.7
4.11 Trusted User Login						
4.11.1AFDI shall require users to login prior to assuming a trusted profile (e.g., system administrator, security officer, root user, super user).	X				DCOIT M	3.2.1.1. 2
4.12 Public Key Infrastructure Functions						
AFDI shall provide the capability to:						
4.12.1Request creation of X.509 certificates in accordance with PKCS #10.				X	DCOIT M	3.2.20.1
4.12.2Receive and store X.509 certificates.				X	DCOIT M	3.2.20.2
4.12.3Request certificate revocation lists (CRL).				X	DCOIT M	3.2.20.3
4.12.4Request third-party X.509 certificates.				X	DCOIT M	3.2.20.4
4.12.5Validate third-party X.509 certificates. Validation of third-party certificates shall include the following:				X	DCOIT M	3.2.20.5
4.12.5.1 Verifying the certificate of the certifying authority of the certificate				X	DCOIT M	3.2.20.5 .1
4.12.5.2 Verifying the certificate chain (i.e., checking the validity dates and signature of the certificate issuer for the original certificate, the issuer's certificate, etc., until a trusted authority is reached)				X	DCOIT M	3.2.20.5 .2
4.12.5.3 Verifying that the certificate nor anything on the certificate chain is on the CRL				X	DCOIT M	3.2.20.5 .3
4.12.5.4 Verifying that the validity period of the certificate has not expired				X	DCOIT M	3.2.20.5 .4
4.12.5.5 Verifying that the certificate is being used for its intended purpose.				X	DCOIT M	3.2.20.. 5
4.12.6AFDI shall provide the capability to create and verify digital signatures. The digital signatures supported by AFDI shall meet the following standards:				X	DCOIT M	3.2.19
4.12.6.1 The Digital Signature Standard (DSS) as specified in FIPS Publication 186				X	DCOIT M	3.2.19.2 .1

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.12.6.2 Rivest, Shamir., and Adleman (RSA) public key cryptography system as specified in Public Key Cryptography Standards (PKCS) #1				X	DCOIT M	3.2.19.2 .2
4.12.7AFDI shall provide the capability to generate public/private keys for both the RSA and DSS.				X	DCOIT M	3.2.20
4.12.8AFDI shall provide the capability to export private keys in accordance with PKCS#12				X	DCOIT M	3.2.19.4
4.12.9AFDI shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital IDs).				X	DCOIT M	3.2.14.1
4.12.10 AFDI shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital IDs).				X	DCOIT M	3.2.14.2
4.13 DAC Checker Function						
This function shall provide the ability to:						
4.13.1Check the discretionary access control permissions assigned to system resources at regular intervals.	X				DCOIT M	
4.13.2Change the access permissions of system resources.	X				DCOIT M	
4.13.3AFDI shall provide the capability to define access between named users and/or defined sets of users and named objects (e.g., files, database elements, and programs).	X				DCOIT M	3.2.5.1
4.13.4AFDI shall provide the capability to control access between named users and/or defined sets of users and named objects (e.g., files, database elements, and programs).	X				DCOIT M	3.2.5.2
4.13.5AFDI shall restrict access to objects based on the user's and/or defined sets of user's identity and on access rights (e.g., read, write, execute).	X				DCOIT M	3.2.5.3
4.13.6AFDI shall provide the capability to restrict access to objects based on the user's role.	X				DCOIT M	3.2.5.3. 1
4.13.7AFDI shall provide the capability to restrict access to objects based on the user's organization.	X				DCOIT M	3.2.5.3. 2
4.13.8AFDI shall provide the capability for users to specify and control sharing of objects by named users or defined sets of users (e.g., UNIX groups, access control lists), or by both.	X				DCOIT M	3.2.5.4
4.13.9AFDI shall provide controls to limit the propagation of access rights.	X				DCOIT M	3.2.5.5
4.13.10 AFDI shall, either by explicit user action or by default, protect objects from unauthorized access.	X				DCOIT M	3.2.5.6
4.13.11 AFDI shall provide the capability to assign access rights to authorized users.	X				DCOIT M	3.2.5.7
4.13.12 AFDI shall permit a user to grant or revoke access to an object if the user has control permission (e.g., file owner) for that object.	X				DCOIT M	3.2.5.9
4.13.13 AFDI shall provide a means to associate applications with a work environment (i.e., profiles) and allow users to specify the work environment (i.e., profile selection) during a session.	X				DCOIT M	3.2.5.9. 1

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.13.14 AFDI shall permit a user to hold membership in multiple groups of users simultaneously and have all the access rights of those groups.	X				DCOIT M	3.2.5.11
4.13.15 AFDI shall be capable of restricting access to input/output (I/O) devices (e.g., floppy disks and tape drives).	X				DCOIT M	3.2.5.11 .1
4.13.16 AFDI shall provide a capability to specify which users may access which I/O devices.		X			DCOIT M	3.2.5.11 .1
4.13.17 The default trusted user(s) shall be the system administrator.	N T	S			DCOIT M	3.2.5.12 .6
4.13.18 AFDI shall provide the capability to control access of mobile code (e.g., Java applets, ActiveX controls) to objects.			X		DCOIT M	3.2.5.13
4.13.19 AFDI shall provide a secure X-display that controls access to X resources by individual. AFDI shall provide the capability to control access to resources based on the following:				X	DCOIT M	3.2.5.14
4.13.19.1 Means of access	S			N T	DCOIT M	3.2.5.15 .1
4.13.19.2 Port (i.e., network protocol) of entry		S		N T	DCOIT M	3.2.5.15 .2
4.13.19.3 Time-of-day	X				DCOIT M	3.2.5.15 .3
4.13.19.4 Day-of-week	X				DCOIT M	3.2.5.15 .4
4.13.19.5 Calendar date range (i.e., 15 June 1997 to 14 June 1998)	S			N T	DCOIT M	3.2.5.15 .5
4.13.19.6 When the screen-lock capability is activated after n minutes, AFDI shall screen-lock the terminal and display a selected screensaver.	X				DCOIT M	3.2.5.16
4.13.20 The configurable time period n shall default to 5 minutes.	X				DCOIT M	3.2.5.16 .1
4.13.21 AFDI shall provide the interface for configuration of screen-lock capabilities by a trusted user (e.g., system administrator).			X		DCOIT M	3.2.5.16 .4
4.13.22 Any user-input device shall be used to initiate actions to restore a screen-locked terminal.	X				DCOIT M	3.2.5.16 .5
4.13.23 The specific input value (whether from keyboard, mouse, or other input device) used to restore a screen-locked terminal shall be ignored except to initiate actions to unlock the terminal. In NT systems, the CTRL-ALT-DEL combination shall unlock the screen and shall not be ignored. That is, pressing and holding the CTRL key shall unlock the screen and shall still be recognized when followed by pressing and holding ALT and pressing DEL.	X				DCOIT M	3.2.5.16 .6
4.13.24 AFDI shall require that users re-authenticate themselves to unlock a screen-locked terminal.	X				DCOIT M	3.2.5.16 .7
4.13.25 The screen-lock capability shall be available for users to activate via icon, menu selection, or button.	X				DCOIT M	3.2.5.16 .8
4.13.26 AFDI shall provide the capability for a trusted user (e.g., system administrator) to unlock a screen-locked terminal irrespective of which user was logged in to that terminal.		X			DCOIT M	3.2.5.16 .9

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.14 User Access Function						
The User Access Function shall:						
4.14.1 Ensure all user keyboard communication with the host and AFDI shall use the ASCII character set.	X				CSE	
4.14.2 Ensure that once the user has access to the system via login, further interactions shall be mediated by a Graphical User Interface (GUI) with commonly recognized attributes.	X				CSE	
4.14.3 Provide an installation utility which shall be prompt-driven and designed to install the AFDI in an operational environment. The Installation Utility shall also provide the ability to install multiple AFDI clients from a centralized workstation.	X				CSE	
4.14.4 Ensure that the AFDI does not require and removes software development tools (e.g. compilers, assemblers, debuggers, CASE tools) from the general user's workstation/server.	X				CSE	
4.14.5 Verify that the operating system installation and configuration is correct (including the required system software) and that each phase of the AFDI installation and configuration has been successfully completed.	X				CSE	
4.14.6 Allow installation of the AFDI on minor releases of a supported operating system	X				CSE	
4.14.7 Configure primary and secondary DNS name servers for each domain.	X				CSE	
4.14.8 provide templates for rules, profile, begin, and finish jumpstart scripts for the Solaris environment only.	X				CSE	
4.14.9 Provide procedures and documentation for the automated installation of Microsoft NT 4.0 workstations.	X				CSE	
4.14.10 Provide procedures and documentation for disk cloning			X		CSE	
4.14.11 Provide procedures and documentation for automated installs of the AFDI product			X		CSE	
4.15 Login Function						
4.15.1 Users must uniquely identify themselves before beginning to perform any actions that the system is expected to mediate. Upon successful user login, AFDI shall display the date and time of the last successful login and the number of unsuccessful login attempts since the last successful login.	X				DCOIT M	3.2.1
4.15.2 AFDI shall enforce individual accountability by providing the capability to uniquely identify each user to the system.	X				DCOIT M	3.2.1.1
4.15.3 AFDI shall require users to uniquely identify themselves before beginning to perform any actions that the system is expected to mediate.	X				DCOIT M	3.2.1.1. 1
4.15.4 AFDI shall require users to login prior to assuming a trusted profile (e.g., system administrator, security officer, root user, super user).	S	? N T			DCOIT M	3.2.1.1. 2
4.15.5 Each user shall be uniquely identifiable (e.g., user name or user ID) within an administrative domain.	X				DCOIT M	3.2.1.2
4.15.6 AFDI shall uniquely identify each user for an entire enterprise	X				DCOIT M	3.2.1.2. 1
4.15.7 AFDI shall provide the capability of associating the user's identity with all auditable actions taken by that individual.	X				DCOIT M	3.2.1.3

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.15.8AFDI shall provide the following mechanism(s) to authenticate each user's identity.	X				DCOIT M	3.2.1.4
4.15.9AFDI shall provide the capability for strong user authentication (i.e., using cryptographically protected authentication or one-time passwords).				X	DCOIT M	3.2.1.4. 4
4.15.10 AFDI shall provide a trusted user the capability to enable or disable display of last successful login date and time and the number of unsuccessful login attempts.				X	DCOIT M	3.2.1.4. 5.1
4.16 System Access (LOGIN) Authentication Function						
4.16.1AFDI shall provide the capability to authenticate each user's identity with a password.	X				DCOIT M	3.2.1.4. 1
4.16.2AFDI shall provide the capability for users, the security officer, and the system to generate passwords.				X	DCOIT M	3.2.1.4. 1.1
4.16.3AFDI shall permit only trusted users to change passwords other than their own.	X				DCOIT M	3.2.1.4. 1.4
4.16.4AFDI shall prevent unauthorized access to authentication data.	X				DCOIT M	3.2.1.5
4.16.5AFDI shall prevent unauthorized disclosure of passwords during transmission across a network.				X	DCOIT M	3.2.1.5. 1
4.16.6AFDI shall prevent unauthorized disclosure of passwords while stored.	X				DCOIT M	3.2.1.5. 2
4.16.7AFDI shall provide the capability to limit invalid login attempts which are indicative of potential login attacks	X				DCOIT M	3.2.1.6
4.16.8If the number of consecutive invalid login attempts for a single user ID reaches a threshold n, where n is configurable by a trusted user, the user ID shall be locked and shall remain locked during all further login attempts with that user ID from within the administrative domain.		X			DCOIT M	3.2.1.6. 1
4.16.9AFDI shall be configurable by a trusted user to provide the capability to set the default number of consecutive login failures.	X				DCOIT M	3.2.1.6. 2
4.16.10 The default number of consecutive login failures shall be three.	X				DCOIT M	3.2.1.6. 2.1
4.16.11 Provide the capability for a trusted user, and only a trusted user, to disable the consecutive login failure functionality.	X				DCOIT M	3.2.1.6. 3
4.16.12 When a user ID is locked, AFDI shall provide the capability to send a notification to a trusted user.	X				DCOIT M	3.2.1.6. 4
4.16.13 Provide the capability for a trusted user to restore locked user IDs.	X				DCOIT M	3.2.1.6. 5
4.16.14 Perform login failure lockout for all login points (e.g., console, remote login) in the administrative domain.		X			DCOIT M	3.2.1.6. 6
4.16.15 Perform login failure lockout for all login points (e.g., console, remote login) in the enterprise.		X			DCOIT M	3.2.1.6. 6.1
4.16.16 Provide a non-forgable, non-replayable distributed authentication mechanism that supports both unilateral (client-to-server) or mutual (client-to-server and server-to-client) authentication.				X	DCOIT M	3.2.1.7

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.16.17 Provide a single sign-on capability that permits access to resources (e.g., applications and information) in a distributed system for which the user is authorized without the user being required to re-authenticate at each host where the resources reside.				X	DCOIT M	3.2.1.8
4.16.18 Provide the capability to restrict the time period for which a user may be permitted to use single sign-on to access resources to n minutes where n is configurable by a trusted user.				X	DCOIT M	3.2.1.8. 1
4.16.19 After n minutes the user shall be required to re-authenticate to access remote resources.				X	DCOIT M	3.2.1.8. 1.1
4.16.20 The default time period n for which a user may be permitted to use single sign-on shall be 480 minutes.				X	DCOIT M	3.2.1.8. 1.2
4.16.21 Support single sign-on using hardware tokens (e.g., smart card, FORTEZZA card as an authentication mechanism during the user's initial login.				X	DCOIT M	3.2.1.8. 2
4.16.22 Support single sign-on using X.509 v3 certificates as an authentication mechanism during the user's initial login.				X	DCOIT M	3.2.1.8. 3
4.16.23 Provide the capability to configure user-based access control for use in a single sign-on implementation, where a single user could be granted access to all or a specific subset of available resources,				X	DCOIT M	3.2.1.8. 4
4.16.24 The system shall support at least three classes of user distinguished by their permitted capabilities: Administrator may use any implemented capability, Trusted User can perform a configured set of administration functions, User can only perform normal functions.	X					
4.16.25 A given user may use the system for one of several purposes, as defined by the administrator. These purposes are defined in sessions which are groups of permitted functions.	X					
4.17 Password Operation Function						
4.17.1AFDI shall provide a graphical user interface (GUI) for changing passwords.	X				DCOIT M	3.2.1.4. 1.1.1
4.17.2General users shall be able generate passwords	X				DCOIT M	3.2.1.4. 1.1
4.17.3The ISSO shall be able generate passwords	X				DCOIT M	3.2.1.4. 1.1
4.17.4The system shall be able generate passwords				X	DCOIT M	3.2.1.4. 1.1
4.17.5AFDI shall provide the capability to authentic each user's identity with a password. Passwords shall meet the following requirements:	X				DCOIT M	3.2.1.4. 1
4.17.6AFDI shall require a password be changed after the age of a password has exceeded a maximum of n days (or weeks) where n is configurable by a trusted user.	X				DCOIT M	3.2.1.4. 1.1.2
4.17.7The default maximum days shall be 91 days.	X				DCOIT M	3.2.1.4. 1.1.2.1
4.17.8AFDI shall provide the capability to notify the user n days (or weeks) prior to password expiration where n is defined by a trusted user.	X				DCOIT M	3.2.1.4. 1.1.2

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.17.9AFDI shall default to notifying the user 7 days (or 1 week) prior to password expiration.	X				DCOIT M	3.2.1.4. 1.1.3
4.17.10 AFDI shall prohibit a password from being changed until the age of a password has exceeded a minimum of n days where n is defined by a trusted user.	X				DCOIT M	3.2.1.4. 1.1.4
4.17.11 The default minimum before a password can be changed shall be 7 days (or 1 week).	X				DCOIT M	3.2.1.4. 1.1.4.1
4.17.12 AFDI shall permit a trusted user to override minimum password age limits when changing passwords.	X				DCOIT M	3.2.1.4. 1.2
4.17.13 When changing the password, AFDI shall prohibit the reuse of the current password and n passwords used prior to the current password where n is defined by a trusted user.	N T		S		DCOIT M	3.2.1.4. 1.3
4.17.14 The default number of prior passwords n shall be 2.	X				DCOIT M	3.2.1.4. 1.3.1
4.17.15 AFDI shall permit only trusted users to change passwords other than their own.	X				DCOIT M	3.2.1.4. 1.4
4.17.16 AFDI shall provide the capability to require users to change a password during the initial use of a password created by trusted users.	X				DCOIT M	3.2.1.4. 1.5
4.17.17 AFDI shall provide the capability to prohibit the use of dictionary words or common passwords.	X				DCOIT M	3.2.1.4. 1.6
4.17.18 AFDI shall provide the capability for a trusted user to include a list of dictionary words or common passwords that are prohibited.	X				DCOIT M	3.2.1.4. 1.6.1
4.17.19 AFDI shall ensure that passwords feature specific characteristics configurable by a trusted user. The following characteristics shall be included:	X				DCOIT M	3.2.1.4. 1.7
4.17.19.1Minimum password length	X				DCOIT M	3.2.1.4. 1.7.1
4.17.19.2The default minimum password length shall be set to eight characters.	X				DCOIT M	3.2.1.4. 1.7.1.1
4.17.19.3Password character set (e.g., alphanumeric plus special American National Standard Code for Information Interchange [ASCII] characters).	X				DCOIT M	3.2.1.4. 1.7.2
4.17.19.4Password includes at least one numeric, case change, or special character (e.g., 0-9, &, %).		X			DCOIT M	3.2.1.4. 1.7.3
4.17.19.5Strings of n repeating characters (e.g., ee), where n is configurable by a trusted user are prohibited.	X				DCOIT M	3.2.1.4. 1.8.1
4.17.19.6AFDI shall default to prohibiting 2 repeating characters.		X			DCOIT M	3.2.1.4. 1.8.1.1
4.17.19.7Use of a user name within a password is prohibited	X				DCOIT M	3.2.1.4. 1.8.2
4.18 Data Security Function						
4.18.1AFDI shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital IDs).				X	DCOIT M	3.2.14.1
4.18.2AFDI shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital IDs).				X	DCOIT M	3.2.14.2
4.19 Object Reuse Function						

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
4.19.1AFDI shall ensure that no information, including encrypted representations of information, produced by a prior subject's actions is made available to any subject that obtains access to an object that has been released back to AFDI.				X	DCOIT M	3.2.10.1
4.19.2AFDI shall ensure that all authorizations to information contained within a storage object have been revoked prior to initial assignment, allocation, or reallocation to a subject from AFDI's pool of unused storage objects.				X	DCOIT M	3.2.10.2
4.20 Data Confidentiality						
4.20.1AFDI shall provide accessible cryptographic application programming interfaces for use by applications to selectively encrypt and decrypt data and files.				X	DCOIT M	3.2.11.1
4.20.2The AFDI shall provide a set of assured APIs capable of accommodating both Type I and Type II Security Services, which can be configured with different security policies.				X	Security SRS	3.2.11.1 .1
4.20.3AFDI shall provide the capability for end-to-end encryption services for user sessions.				X	DCOIT M	3.2.11.2
4.20.4AFDI shall provide end-to-end encryption using a unique private key for each user.				X	DCOIT M	3.2.11.2 .1
4.20.5AFDI shall protect the confidentiality and integrity of user private keys.				X	DCOIT M	3.2.11.2 .2
4.20.6AFDI shall provide the capability for a user to transport his or her private key from one user platform to another user platform.				X	DCOIT M	3.2.11.2 .3
4.20.7AFDI shall provide the capability for key recovery.				X	DCOIT M	3.2.11.3
4.20.8AFDI shall provide an Internet Protocol Security (IPSEC) encryption capability as defined in the Internet Protocol, Version 6 (Ipv6) Specification (Deering, 1997).				X	DCOIT M	3.2.11.4
4.20.9AFDI shall provide an administrative interface that allows a security officer to manage the IPSEC Security Policy Database (SPD) as defined in the <i>Security Architecture for the Internet Protocol</i> (Kent, 1998).				X	DCOIT M	3.2.11.4 .1
5.0 Account Management						
5.1 Account Creation Function						
5.1.1 AFDI shall provide the capability for centralized user account <i>creation</i> in a heterogeneous environment with the capability to define the following user parameters:	X				ADMS RS	3.2.1.19
5.1.1.1 Unique user identifier (within administrative domain)	X				ADMS RS	3.2.1.19
5.1.1.2 Login name	X				ADMS RS	3.2.1.19
5.1.1.3 Initial password in accordance with the Security SRS	X				ADMS RS	3.2.1.19
5.1.1.4 Automatic password generation in accordance with the Security SRS				X	ADMS RS	3.2.1.19
5.1.1.5 Home directory path	X				ADMS RS	3.2.1.19
5.1.1.6 Login directory path	X				ADMS RS	3.2.1.19

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
5.1.1.7 Password expiration in accordance with Security SRS	X				ADMS RS	3.2.1.19
5.1.1.8 Default profile			X		ADMS RS	3.2.1.19
5.1.1.9 Home directory file server	X				ADMS RS	3.2.1.19
5.1.1.10 Group memberships	X				ADMS RS	3.2.1.19
5.1.1.11 Mail alias(es)	X				ADMS RS	3.2.1.19
5.1.1.12 Mail destination		X			ADMS RS	3.2.1.19
5.1.1.13 Shell	X				ADMS RS	3.2.1.19
5.1.1.14 Other user information, e.g., user's real name, telephone	X				ADMS RS	3.2.1.19
5.1.2 The user account creation mechanism shall provide an API or equivalent mechanism that shall support the execution of additional tasks during user account creation as required by AFDI and its segments. These tasks may include adding users to the DBMS, Profile Database and creating the user's home directory.	S			N T	ADMS RS	3.2.1.20
5.1.3 AFDI shall create users such that it shall support single sign-on of the user in accordance with the Security SRS.				X	ADMS RS	3.2.1.21
5.1.4 AFDI shall provide a single sign-on capability to support transparent, distributed login for all users in accordance with the Security SRS.				X	ADMS RS	3.2.1.22
5.1.5 AFDI shall provide the capability for centralized user account <i>modification</i> in a heterogeneous environment with the capability to modify the specified user parameters, at a minimum:	X				ADMS RS	3.2.1.23
5.1.5.1 Login name	X				ADMS RS	3.2.1.23
5.1.5.2 Password	X				ADMS RS	3.2.1.23
5.1.5.3 Home directory file server	X				ADMS RS	3.2.1.23
5.1.5.4 Group memberships	X				ADMS RS	3.2.1.23
5.1.5.5 Mail alias(es)	X				ADMS RS	3.2.1.23
5.1.5.6 Shell	X				ADMS RS	3.2.1.23
5.1.5.7 Other user information, e.g., user's real name, telephone	X				ADMS RS	3.2.1.23
5.1.6 If the user's home directory file server is modified, the account modification mechanism shall create a new home directory on that server.			X		ADMS RS	3.2.1.23

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
5.1.7 AFDI shall provide the capability for centralized user account deletion in a heterogeneous environment. The user account deletion mechanism shall provide the capability to reverse all actions associated with user account creation. The account deletion mechanism shall prompt for user home directory deletion, with a default of “no”.	X				ADMS RS	3.2.1.24
5.1.8 The user account deletion mechanism shall be extensible such that it shall support the execution of additional tasks during user account deletion as required by AFDI and its segments. These tasks may include deleting users from the DBMS, Profile Database and deleting the user’s home directory.	S			N T	ADMS RS	3.2.1.25
5.1.9 AFDI shall provide the capability for centralized group creation in a heterogeneous environment with the capability to modify the following <i>group parameters</i> :	X				ADMS RS	3.2.1.27
5.1.9.1 Unique group identifier (within administrative domain)	X				ADMS RS	3.2.1.27
5.1.9.2 Group name	X				ADMS RS	3.2.1.27
5.1.9.3 Members	X				ADMS RS	3.2.1.27
5.1.10 AFDI shall provide the capability for centralized group modification in a heterogeneous environment with the capability to modify the following <i>group parameters</i> :	X				ADMS RS	3.2.1.28
5.1.10.1 Group ID	X				ADMS RS	3.2.1.28
5.1.10.2 Group Name	X				ADMS RS	3.2.1.28
5.1.10.3 Members	X				ADMS RS	3.2.1.28
5.1.11 AFDI shall provide the capability for centralized group deletion in a heterogeneous environment. The group account deletion mechanism shall provide the capability to reverse all actions associated with group account creation.	X				ADMS RS	3.2.1.29
5.1.12 AFDI shall provide the capability to automatically distribute or make available via network information services group information to a single host, a group of hosts or all hosts within the administrative domain.	X				ADMS RS	3.2.1.30
Account Management capabilities shall include:						
5.1.13 Identifying types of accounts (individual and group, conditions for group membership, associated privileges).	X				DCID 6/3	
5.1.14 Establishing an account (i.e., required paperwork and processes).	X				DCID 6/3	
5.1.15 Activating an account.	X				DCID 6/3	
5.1.16 Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).	X				DCID 6/3	
5.1.17 Terminating an account (i.e., processes and assurances).	X				DCID 6/3	
5.2 Account Management Function						
AFDI shall allow a trusted user to perform the following capabilities:						

S = Solaris Only
NT = NT Only

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.X	Doc.	Para.
5.2.1 Administer User Account Maintenance and Administrative Maps	X				CSE	
5.2.2 Create a User Account	X				CSE	
5.2.3 View User Account Information	X				CSE	
5.2.4 Modify User Account Information	X				CSE	
5.2.5 Clear Locked Accounts and Failed Logins	X				CSE	
5.2.6 Remove a user account	X				CSE	
5.2.7 Enable/disable user account	X				CSE	
5.2.8 Assign user passwords	X				CSE	
6.0 Testing						
6.1 For DCID 6/3 Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.	X				DCID 6/3	
6.2 A test plan and procedures shall be developed and include:	X				DCID 6/3	
6.2.1 A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.	X				DCID 6/3	
6.2.2 A detailed description of the assurances that have been implemented, and how this implementation shall be verified.	X				DCID 6/3	
6.2.3 An outline of the inspection and test procedures used to verify this compliance.	X				DCID 6/3	