Complete System Administrator Checklist

Daily			
Area	**Tasks**	**Status**	**Notes**
Review Audit logs	Check application log for warning and error messages for service startup errors, application or database errors and unauthorized application installs		
	Check security log for warning and error messages for invalid logons, unauthorized user creating, opening or deleting files		
	Check system log for warning and error messages for hardware and network failures		
	Check web/database/application logs for warning and error messages		
	Check directory services log on domain controllers		
	Report suspicious activity to IAO		
Perform/verify daily backup	Run and/or verify that a successful backup of system and data files has completed		
	Run and/or verify that a successful backup of Active Directory files has completed on at least one Domain Controller		
Track/monitor system performance and activity	Check for memory usage		
	Check for system paging		
	Check CPU usage		
Check free hard-drive space	Check all drives for adequate free space		
	Take appropriate action as specified by site's Standard Operating		
Physical checks of system	Visually check the equipment for amber lights, alarms, etc.		
	Take appropriate action as specified by site's Standard Operating		
Weekly			
Archive Audit logs	Archive audit logs to a media device with one year retention		
Perform/verify weekly backup	Run or verify that a successful backup of system and data files has been completed		
Update Anti-Virus signature file	Download and install current Anti-Virus signature files		
Run Anti-Virus scan on all hard-drives	Scan all hard-drives using current Anti-Virus signature files		

Check Vendor Websites for Patch Information	Check vendor websites such as Microsoft, Sun, HP, Oracle, etc for new vulnerability information including patches and hotfixes		
Compare system configuration files against a baseline for changes	Compare system configuration files against the baseline		
	Compare application executables against the baseline		
	Compare database stored procedures against the		
Run file system integrity diagnostics	Run diagnostic tools to detect any system problems		
Verify Retina Vulnerability Scan Performed (SCCVI)	Verify system scanned by IAO or NSO using Retina tool to detect for vulnerabilities		
Remediate with Citadel Hercules remediation Tool (SCRI)	Verify Hercules remediation tool is used on system to correct vulnerabilities		
Check for Password Files	Perform file search on system checking for documents containing words such as 'password', 'passwd', 'pwd', etc		
Perform Wireless Check	Check system for wireless devices and access		
Perform server clock/time synchronization	Synchronize system clock with master server		
	References		
Check for Unnecessary Services	Check system services for any unnecessary services running		
Monthly			
Perform Self-Assessment Security Review	Review technology checklist for any changes		
	Run current security review tool		
	Import results into Vulnerability Management System (VMS)		

Perform Hardware/Software Inventory	Review hardware and compare to inventory list		
	Review software and compare to inventory list		
	Update VMS, where applicable		
Run Password-Cracking Tool (Domain Controller only)	Run (or verify IAO team has run) a password-cracking tool to detect weak passwords		
	Provide output to IAO team		
Perform/verify monthly backup	Run or verify that a successful backup of system and data files has been completed		
Verify User Account Configuration	Run DumpSec tool to verify user account configuration		
	Verify and/or delete dormant accounts with IAO		
	Provide output to IAO team		
Quarterly			
Test backup/restore procedures	Restore backup files to a test system to verify procedures and files		
Annually			
Change Service-Account passwords	Work with appropriate application administrator to ensure password changes for service accounts such as database accounts, application accounts and other service accounts are implemented		
Review appropriate Security Technical Implementation Guides (STIG)	Review appropriate STIGs which are updated annually		

Participate in STIG Technical Interchange Meetings (TIM), when possible	Participate in TIMs to exchange information about updated STIGs, etc.		
Review training requirements	Review training requirements according to DoD Directive 8570.1		
As Required	Test Patches and Hotfixes		
	Install Patches and Hotfixes		
	Schedule Downtime for Reboots		
	Apply OS upgrades and service packs		
	Create/maintain user and groups accounts		
	Set user and group security		
After system configuration changes:	Create Emergency System Recovery Data		
	Create new system configuration baseline		
	Document System Configuration Changes		
	Review and update SSAA		
	Update VMS for Asset Changes		
	Update VMS for IAVMs		

Tools	**References**
Windows Event Viewer	
Windows Backup Tool	
Veritas Backup Software	
Microsoft Management Console	www.Microsoft.com - Monitoring Server performance
Performance Log and Alerts	
Task Manager	
System Monitor	
Microsoft Operations Manager	
Disk Defragmenter	www.Microsoft.com - Monitoring Server performance
Disk Management	
Disk Quotas	
Windows Backup Tool	
Veritas Backup Software	
	www.cert.mil

	http://iase.disa.mil - DoD Patch Repository
	www.cert.mil
Unix Tripwire	
Disk Defragmenter	www.Microsoft.com - Managing Disks and Volumes
Error-checking	
Device Manager	
	http://iase.disa.mil - DoD IA Enterprise-wide Tools and Software: SCCVI
	(DoD PKI cert req'd)
	http://iase.disa.mil - DoD IA Enterprise-wide Tools and Software: SCCVI
	(DoD PKI cert req'd)
	http://iase.disa.mil - Security Technical Implementation Guides (STIGs)
Windows Time Service	www.Microsoft.com - Windows Time Service
Tools - Unix /Windows	
NTP	
DISA FSO Gold Disk and Scripts	http://iase.disa.mil - DoD IA Enterprise-wide Tools and Software:
eEye Retina Scanner	Gold Disk (.mil only)
Citadel Hercules Remediation Tool	http://iase.disa.mil - IA Subject Matter Areas: Security Technical

Tools - UNIX	Implementation Guides - STIGS: Security Readiness Review Evaluation Scripts
DISA FSO Scripts	
eEye Retina Scanner	
Citadel Hercules Remediation Tool	
John-the-Ripper	
L0phtCrack	
Tools - UNIX	
Crack	
Tools available on DISA FSO Gold Disk (Windows) and	
DISA FSO Scripts (UNIX)	
Windows Backup Tool	
Veritas Backup Software	
Tool available on DISA FSO Gold Disk (Windows)	
Windows Backup and Recovery Tool	
Veritas Backup Software	

	http://iase.disa.mil - IA Subject Matter Areas: Policy and Guidance