

**Joint System Administrator Checklist**  
**Version 1.1**  
**22 December 2005**

**Daily**

**Review Audit logs**

**Tasks**

- 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

**References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

**Tools – Windows**

Event Viewer

**Perform/verify daily backup**

**Tasks**

- 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

**References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

**Tools**

Windows Backup Tool  
Veritas Backup Software

**Track/monitor system performance and activity**

**Tasks**

- Check for memory usage
- Check for system paging
- Check CPU usage

**References**

[www.Microsoft.com](http://www.Microsoft.com) - Monitoring Server performance

**Tools – Windows**

Microsoft Management Console  
Performance Log and Alerts

Task Manager  
System Monitor  
Microsoft Operations Manager

### **Check free hard-drive space**

#### **Tasks**

Check all drives for adequate free space  
Take appropriate action as specified by site's Standard Operating Procedures

#### **References**

[www.Microsoft.com](http://www.Microsoft.com) - Monitoring Server performance

#### **Tools – Windows**

Disk Defragmenter  
Disk Management  
Disk Quotas

### **Physical checks of system**

#### **Tasks**

Visually check the equipment for amber lights, alarms, etc.  
Take appropriate action as specified by site's Standard Operating Procedures

## **Weekly**

### **Archive Audit logs**

#### **Tasks**

Archive audit logs to a media device with one year retention

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Perform/verify weekly backup**

#### **Tasks**

Run or verify that a successful backup of system and data files has been completed

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

#### **Tools**

Windows Backup Tool  
Veritas Backup Software

### **Update Anti-Virus signature file**

#### **Tasks**

Download and install current Anti-Virus signature files

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

#### **Downloads**

[www.cert.mil](http://www.cert.mil)

### **Run Anti-Virus scan on all hard-drives**

#### **Tasks**

Scan all hard-drives using current Anti-Virus signature files

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Check Vendor Websites for Patch Information**

#### **Tasks**

Check vendor websites such as Microsoft, Sun, HP, Oracle, etc for new vulnerability information including patches and hotfixes

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

#### **Downloads**

<http://iase.disa.mil> – DoD Patch Repository  
[www.cert.mil](http://www.cert.mil)

### **Compare system configuration files against a baseline for changes**

#### **Tasks**

Compare system configuration files against the baseline  
Compare application executables against the baseline  
Compare database stored procedures against the baseline

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

#### **Tools – Unix**

Tripwire

### **Run file system integrity diagnostics**

#### **Tasks**

Run diagnostic tools to detect any system problems

#### **References**

[www.Microsoft.com](http://www.Microsoft.com) - Managing Disks and Volumes

#### **Tools – Windows**

Disk Defragmenter  
Error-checking tool  
Device Manager

### **Verify Retina Vulnerability Scan Performed (SCCVI)**

#### **Tasks**

Verify system scanned by IAO or NSO using Retina tool to detect for vulnerabilities

#### **Downloads**

<http://iase.disa.mil> – DoD IA Enterprise-wide Tools and Software: SCCVI  
(DoD PKI cert req'd)

## **Remediate with Citadel Hercules remediation Tool (SCRI)**

### **Tasks**

Verify Hercules remediation tool is used on system to correct vulnerabilities

### **Downloads**

<http://iase.disa.mil> – DoD IA Enterprise-wide Tools and Software: SCCVI  
(DoD PKI cert req'd)

## **Check for Password Files**

### **Tasks**

Perform file search on system checking for documents containing words such as 'password', 'passwd', 'pwd', etc

## **Perform Wireless Check**

### **Tasks**

Check system for wireless devices and access

### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

## **Perform server clock/time synchronization**

### **Tasks**

Synchronize system clock with master server

### **References**

[www.microsoft.com](http://www.microsoft.com) – Windows Time Service

### **Tools – Windows**

Windows Time Service

### **Tools – Unix /Windows**

NTP

## **Check for Unnecessary Services**

### **Tasks**

Check system services for any unnecessary services running

### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

## **Monthly**

### **Perform Self-Assessment Security Review**

#### **Tasks**

Review technology checklist for any changes

Run current security review tool

Import results into Vulnerability Management System (VMS)

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

<https://vms.disa.mil>

## **Downloads**

<http://iase.disa.mil> – DoD IA Enterprise-wide Tools and Software:  
Gold Disk (.mil only)

<http://iase.disa.mil> – IA Subject Matter Areas: Security Technical  
Implementation Guides – STIGS: Security Readiness Review  
Evaluation Scripts

### **Tools – Windows**

DISA FSO Gold Disk and Scripts  
eEye Retina Scanner  
Citadel Hercules Remediation Tool

### **Tools – UNIX**

DISA FSO Scripts  
eEye Retina Scanner  
Citadel Hercules Remediation Tool

## **Perform Hardware/Software Inventory**

### **Tasks**

Review hardware and compare to inventory list  
Review software and compare to inventory list  
Update VMS, where applicable

### **References**

<https://vms.disa.mil>

## **Run Password-Cracking Tool (Domain Controller only)**

### **Tasks**

Run (or verify IAO team has run) a password-cracking tool to detect  
weak passwords  
Provide output to IAO team

### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Tools – Windows**

John-the-Ripper  
L0phtCrack

### **Tools - UNIX**

Crack

**Tools available** on DISA FSO Gold Disk (Windows) and  
DISA FSO Scripts (UNIX)

## **Perform/verify monthly backup**

### **Tasks**

Run or verify that a successful backup of system and data files has been  
completed

### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Tools**

Windows Backup Tool  
Veritas Backup Software

### **Verify User Account Configuration**

#### **Tasks**

Run DumpSec tool to verify user account configuration  
Verify and/or delete dormant accounts with IAO approval  
Provide output to IAO team

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

**Tool available** on DISA FSO Gold Disk (Windows)

## **Quarterly**

### **Test backup/restore procedures**

#### **Tasks**

Restore backup files to a test system to verify procedures and files

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

#### **Tools**

Windows Backup and Recovery Tool  
Veritas Backup Software

## **Annually**

### **Change Service-Account passwords**

#### **Tasks**

Work with appropriate application administrator to ensure password changes for service accounts such as database accounts, application accounts and other service accounts are implemented

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Review appropriate Security Technical Implementation Guides (STIG)**

#### **Tasks**

Review appropriate STIGs which are updated annually

#### **References**

<http://iase.disa.mil> - Security Technical Implementation Guides (STIGs)

### **Participate in STIG Technical Interchange Meetings (TIM), when possible**

#### **Tasks**

Participate in TIMs to exchange information about updated STIGs, etc.

#### **References**

<http://iase.disa.mil>

## **Review training requirements**

### **Tasks**

Review training requirements according to DoD Directive 8570.1

### **References**

<http://iase.disa.mil> – IA Subject Matter Areas: Policy and Guidance

## **Initial**

### **Subscribe to STIG News**

#### **Reference**

<http://iase.disa.mil/request-mail.html>

### **Subscribe to JTF-GNO Mailings**

#### **Reference**

<ftp://ftp.cert.mil/pub/misc/subscribe.htm>

## **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**

### **Subscribe to STIG News**

### **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**

Point of Contact for Document: [fso\\_spt@disa.mil](mailto:fso_spt@disa.mil)

Document Location: <http://iase.disa.mil>

Incident Notification: Contact Site IAO