

## Best Pick: IT Security Tools

**Purpose:** The purpose of this document is to identify best security tools, identified by agencies responsible for protecting federal taxpayer information. This applies to the Internal Revenue Service and all state agencies that are responsible for implementing the security controls for information systems, where Federal Tax Information (FTI) is stored, transmitted, or processed.

**Background:** The Tactical Advisory Group (TAG) Security Subgroup (SS) was established to develop security solutions for systemic security problems. While some agencies struggle to implement strong security controls, other agencies have procured software that enables the IT security controls to be better managed. This list of controls is identified within this document.

By reviewing this list, agencies may determine if there are new solutions or better solutions that will enable them to protect FTI. By using any of these tools, this will not guarantee a passing and/or failing grade for any upcoming Safeguard Reviews. By implementing these controls, an organization will be better postured in the entire area of IT security.

**Recommended Use:** To ensure state taxation agencies implement security controls effectively, the TAG SS recommends that managers review the security control areas, such as access control. At this point, determine if your agency has effective management tools. If not, you may use this list to evaluate tools other agencies have identified as effective.

**Version #:** 1.0, dated September 1, 2006

**Questions:** Questions regarding this document may be addressed to [ellen.o.pieklo@irs.gov](mailto:ellen.o.pieklo@irs.gov). Any questions and/or feedback will then be forwarded to the TAG SS for archival purposes.

## Best Pick: IT Security Tools

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
Access Controls & Auditing	Active Directory	Windows	-	FTB
Access Controls & Auditing	Aelita/Quest Journal	Windows	<a href="http://www.quest.com">www.quest.com</a> has a variety of tools for system, application and database administration.	IRS
Access Controls & Auditing	Aelita/Quest Reporting Console	Windows	<a href="http://www.quest.com">www.quest.com</a> has a variety of tools for system, application and database administration.	IRS
Access Controls & Auditing	Aelita/Quest Repository Viewer	Windows	<a href="http://www.quest.com">www.quest.com</a> has a variety of tools for system, application and database administration.	IRS
Access Controls & Auditing	Blue Coat	Appliance	HTTP control and logging	FTB
Access Controls & Auditing	Finjan	Appliance	Malicious Active Content	FTB
Access Controls & Auditing	Top Secret	IBM zOS	For Mainframe	KS,FTB
Access/Authentication	Microsoft W2000 Radius Server	Windows	To authenticate External VPN Clients to Windows domain	KS
Access/Authentication	Microsoft W2000 Radius Server	Windows	To authenticate External VPN Clients to Windows domain	KS
Account and Administration Management of Active Directory	WebAD		Quest ActiveRoles Server Web Interface that facilitates the administration and provisioning of accounts in Active Directory.	IRS
Auditing	Aelita Quest Event Admin	Windows	<a href="http://www.quest.com">www.quest.com</a> has a variety of tools for system.	IRS

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
			<a href="#">application and database administration.</a>	
Auditing	Check Point	Nokia Appliance	Firewall logs	FTB,KS
Auditing	Enterprise Security Manager	Windows	Provides oversight over Windows NT/XP domains	IRS
Auditing	Aelita (InTrust, Quest Reporter)	Windows	<a href="http://www.quest.com">www.quest.com</a> has a variety of tools for system, application and database administration. Validates user access, reports on events	IRS
Auditing	Enterprise Directory Reporter	Windows		IRS,CT
Auditing	Network Intelligence	Appliance	Audit log aggregation	FTB
Configuration Management	ESM STAR report:	Windows	Providing statistics on: COE versioning, NAV versioning, IE Versioning, OS versioning, Identity Management (DIRECT) compliance, Outlook Versioning	IRS
Disaster Recovery/ Business Resumption	Veritas Backup	Windows	Allows backup of system to be made	IRS,FTB
Disaster Recovery/ Business Resumption	Veritas Backup ArcServ 11.1	UNIX	Allows backup of system to be made	KS
Disaster Recovery/ Business Resumption	Legato		System backups	FTB
Domain administration	Active Directory	Windows		FTB

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
Domain Administration	Hyena <a href="http://www.systemtools.com/">http://www.systemtools.com/</a>	Microsoft	Windows NT/2000/2003/XP System Administration Software	Wisconsin DOR
Domain administration	IBM Manager	Windows	Part of Windows Enterprise Security Manager	IRS
Domain administration	Insight Manager	Windows	Part of Windows Enterprise Security Manager	IRS
Domain administration	Net IQ App Manager	Windows	Part of Windows Enterprise Security Manager	IRS
Domain Administration	NETIQ App Manager	Windows	System monitoring for Active Directory, Exchange 5.5 and 2003, Server Management and Monitoring	IRS
Domain Administration	NETIQ GPA	Windows: Active Directory	Used to verify the specific GPO settings and the linkage of the OU(Organizational Unit ) linked to the GPO. Configuration Management tool for the GPO's . Can be used across multiple domains/forests.	IRS
Firewall	Checkpoint NGR 5.5	Network	Provide Firewall for the Network	KS
Firewall	Microsoft ISA Server	Network	Proxy Authentication for Internet Access	KS
Group management	showmbrs.exe	Windows: Active Directory	This command-line tool shows the user names of members of a given group, even within a given network domain.	IRS
IDS/IPS	ISS Real Secure	Windows	Host & Network Intrusion Detection and Prevention	KS

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
Inventory Management	HP Insight Manager	Windows	Hardware - Software management and monitoring. These include: Inventory Management, Fault Management, Remote Management, Blade System management	IRS, FTB
Inventory Management	In-House Application	Windows	Inventory Management	KS
Inventory Management	Track-It	Windows	Track hardware and software inventory	FTB
Media Management: Disk Overwrite Tools	DataGone	Windows		FTB
Media Management: Disk Overwrite Tools	Symantec Ghost 7.5	Windows	Allows disk drives to be overwritten so data cannot be recovered	IRS, KS (Ghost 8.1), CT
Patch Management	Altiris Patch Management	Windows	Mmanage MS hotifx distributions on WINTEL servers	IRS
Patch Management	BigFix	Windows, AIX, HP-UX		FTB
Patch Management	ESM Configuration Management	Windows	Performs automated distributions of Hotfix	IRS
Patch Management	ESM Patch Management	Windows	Automated ESM MBSA reporting on patch deficiencies on servers and workstations across the enterprise on a bi-weekly cycle.	IRS
Patch Management	HFnetchk	Windows	Shavlik's HFNetChk freeware patch scanning utility - checks for latest patches	IRS, FTB

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
Patch Management	MBSA2.0		To determine server compliance level and security settings. Identifies missing patches. Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed to determine the security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems. Scripts can be created to check multiple systems using this tool.	IRS,FTB
Patch Management	MITSDATA Version 7.3.0		machines are not up to the latest COE, old Virus Defs, old VirusScan software, Duplicate TSIDS, missing M2 Patches, machine mhz MITSDATA is a program that lets you scan and create canned queries/reports for COE, NAV, etc	IRS
Patch Management	MSBA Microsoft Security Baseline Analyzer	Windows	checks for latest patches	IRS,FTB,CT
Patch Management	Tivoli	Windows	Manages software on systems	IRS

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
Patch Management and reporting	Altiris Server Suite Management	Windows	Deploys patches to servers and generates online reports on patch compliance. Server software monitoring and reports the compliance levels for Microsoft patches currently.	IRS
Patch Reporting	MBSA1.2.1		To determine server compliance level and security settings. Identifies missing patches. Also is currently a component within LEM Checker 2.2.	IRS
Patch Reporting	Nessus	Linux	Vulnerability scanner	FTB
Router & Switch Management	CSIRC Penetration Test	Routers/Switches	Monitor compliance with SANS top 20. Identifies instances of blank passwords	IRS
Router & Switch Management	CSIRC Vulnerability Test	Routers/Switches	Monitor compliance with SANS top 20. Looks for common security misconfigurations	IRS
Router & Switch management	<u>TACACS (protocol)</u>	Routers & Switches	Allows router & Switch management of Cisco devices	IRS,KS(DISC),FTB
Router and Switch Configuration Management	<u>Cisco Secure (product)</u>	Routers/Switches	Provides centralized access control management to Cisco routers and switches and does event logging.	IRS,KS(DISC),FTB
Router and Switch Configuration Management	Cisco Security Analyzer	Routers/Switches	Can use OPNET NetDoctor instead of Cisco Security Analyzer for reviewing router and switch configurations. Validates the configuration of Cisco	IRS,FTB

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
			routers and switches	
Router and Switch Configuration Management	Cisco Works	Routers/Switches	Records access to routers and switches. Used to manage router and switch configurations. Event logging.	IRS,FTB
Router and Switch Configurations	Net Doctor	Routers/Switches	OPNET NetDoctor automatically reviews router and switch configurations for compliance with router and switch policies	IRS
Router Management	Opnet ACE agent 2.4.	Routers/Switches		IRS
Router Management	Opnet ACEagent light	Routers/Switches	facilitate network and application troubleshooting	IRS
Secure Email	Tumbleweed	Windows	To encrypt email that has confidential info	KS
SPAM Management	McAfee Spam Killer	Windows	SPAM Management	KS
SPAM Management	Tumbleweed	Windows	SPAM Management	KS
Tool Kit, part of Resource Kit	local.exe	Windows	Windows NT 4.0 Resource Kit Supplement 4. Local Groups	IRS,KS
UNIX	Computer Associates eTrust Audit	Unix	As currently deployed, consolidates reports from various eTrust Access Control instances for consolidated Solaris Unix configuration file reporting.	IRS, KS-CA Security

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
User and account administration	net.exe	Windows	Command-line tool Net command-line tool allows you to manage the local user database, start and stop services, and connect to shared folders.	IRS,KS
Virus and SPAM Management	ProofPoint	Appliance	SMTP SPAM blocker	FTB
Virus and SPAM Management	Sabari Antigen	Windows	Exchange Anti-virus	FTB
Virus and SPAM Management	Symantec	Windows	Workstation and Server Anti-virus	FTB
Virus and SPAM Management	Symantec Anti-Spam	Windows	Controls incoming Spam into the environment	IRS
Virus and SPAM Management	TrendMicro	Windows	Exchange Anti-virus	FTB
Virus Management	McAfee EPO	Windows	To automatically distribute dat file anti-virus updates	KS
Windows Patch & Updated component	WSUS	Windows	Microsoft Windows Server Update Services (WSUS) Windows Server Update Services is a patch and update component of Windows Server	IRS,KS,FTB
Windows Security Management	Dumpsec	Windows	SomarSoft's DumpSec is a security auditing program for Microsoft Windows® NT/XP/200x. It dumps the permissions (DACLS) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent.	IRS

Compliance Function	Access Control Tools	Environment Supported	How Are They Used?	Agencies/State Using Tools
			DumpSec also dumps user, group and replication information. Used to produce a list of all users and their last TRUE logon.	