



Web Farm Security Assessment Guide

June 18, 2002

FINAL DRAFT

Prepared by:
Barre Bull, Technical Director for Information
Security Services, Project Manager
Nikita Black, IT Security Analyst



13921 Park Center Road, Suite 300,
Herndon, VA 20171

SAIC-6663-2002-188

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Web Farm Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Web Servers within USDA Web Farms. This checklist is *not intended to be a configuration guide* but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. This checklist should be used in conjunction with the appropriate system checklist to determine the overall security stature of the systems within the web farm. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU systems.

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, and "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements.

4. REFERENCES

a. External

- (1) Public Law 100-235, "Computer Security Act of 1987"
- (2) Public Law 93-579, "Privacy Act of 1974"
- (3) Public Law 93-502, "Freedom of Information Act"
- (4) Public Law 99-474, "Computer Fraud and Abuse Act"
- (5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
- (6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.
- (7) FIPS Pub 140-2, "Security Requirements for Cryptographic Modules" May 25, 2001.

b. USDA Internal Regulations

- (1) DR 3140-001, "USDA Information Systems Security Policy" dated May 15, 1996.
- (2) DM 3140-1 "USDA Management ADP Security Manual" dated March 5, 1992.

Web Farm Security Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Based upon the requirement, answer all questions as "Yes", "No", "Partial", or "N/A (Non-applicable)". Provide supplemental information as appropriate. All "No", and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be completed by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency Identification:

Agency (Agency, Office, Bureau, Service, etc.):		
Address		
ISSPM		Phone:
Date of last Assessment:		

Test Number: 1	SYSTEM:	DATE:	TIME:
Test Name: Web and FTP Server General Security			
Resources Required:	Access to the Web and FTP servers within the web farm.		
Personnel Required:	System Administrator or Web/FTP Server Administrator		
Objectives:	To determine that the Web and FTP servers within the web farm are configured to meet USDA requirements pertaining to internet system protections, user access privileges, and network security.		
Procedure Description: (Summary)	Verify that access is properly controlled. Verify that the servers are run with as little privilege as necessary. Verify that server functionality is executed in a restricted file space. Verify that system integrity is monitored and maintained.		

Detailed Procedures and Results

Step #	Procedure Description Web and FTP Server General Security	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
1.	Has a perimeter security solution that includes firewalls and intrusion detection, been implemented to protect the systems within the Web Farm?	A perimeter security solution that includes firewalls and intrusion detection has been implemented to protect the systems within the Web Farm.		
2.	Is security layered according to the value of the server contents?	Security is layered according to the value of the server contents. Consider layering multiple tiers of security in accordance with the value of the server contents.		
3.	Is the Web server configured with appropriate controls to protect it from unauthorized access and misuse? Are the appropriate physical security measures in place?	The Web server is configured with appropriate controls to protect it from unauthorized access and misuse. The web server should be configured with appropriate object, device, and file access controls. Physical security measures required to protect the web server(s) are in place.		
4.	Are Web and FTP servers run on the same machine?	Web and FTP servers are run on different/separate machines. Web and FTP servers should not be on the same machine.		
5.	Are the test and production web servers periodically tested (ex. System scans) for vulnerabilities in accordance with USDA policy?	The Web servers are periodically tested for vulnerabilities in accordance with USDA policy.		

Step #	Procedure Description Web and FTP Server General Security	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
6.	Is intrusion detection software installed on the system?	Intrusion detection software is installed on the system. Intrusion detection software should be installed to monitor server connections and to detect exploits and suspicious activities.		
7.	Is the number of persons having administrator or root level access limited and documented?	The number of persons having administrator or root level access is limited and documented according to business requirements.		
8.	Are remote administration tools, such as System Policy Editor, Registry Editor, System Monitor and Net Watcher installed or active on the web server?	Remote administration tools or web pages are not installed or active on the web server These tools/web pages should not be installed or active. If installed or active, make sure that they are appropriately protected. For example, access should only be made available via an authenticated encrypted session.		
9.	Are remote access connections used to administer web servers secure?	Remote access connections used to administer web servers are secure. Remote administrative connections should be secured, either via token-based identification, virtual private network encryption or Secure Shell encryption.		
10.	Is administrative access to systems physically restricted?	Administrative access to the externally visible or key elements of the server is physically restricted.		
11.	Is administrative access logically restricted?	Administrative access to the externally visible or key elements of the server is logically restricted.		
12.	Are functionality or Internet services such as telnet, email SMTP, IMAP, POP, FTP, CHAT, NNTP, LDAP directory services identified, appropriately authorized, protected and managed?	Internet services such as telnet, email, FTP, CHAT, NNTP, LDAP directory services have been identified and are appropriately authorized, protected and managed. These services should be identified, authorized, protected and managed, under the same security arrangements that apply to the core server services.		
13.	Are unused services such as FTP, the r services (rlogin, rsync), TFTP, etc. disabled?	Unused services such as FTP, the r services, TFTP, etc. are disabled? Default services, especially FTP and Telnet, leave the system vulnerable. Keep FTP only if needed and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.		

Step #	Procedure Description Web and FTP Server General Security	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
14.	Are Web-server-specific logging mechanisms for both the server and web server identified and implemented?	Web-server-specific logging mechanisms for both the server and web server application(s) have been identified and are implemented.		
15.	Is user activity, such as logins and system transactions, logged and maintained in an encrypted form and stored in a secure location?	All user activity is logged and maintained either in an encrypted form on the web server or stored on a separate machine on the Intranet.		
16.	Are log files reviewed on a regular basis?	Log files are reviewed on a regular basis according to sensitive resources.		
17.	Are content updates performed only from the Intranet?	Content updates are performed only from the Intranet. Do all updates from the Intranet. Maintain web page originals on an Intranet server and make all changes and updates there. Push updates to the public server.		
18.	Are patches, upgrades, and operating system software up-to-date and supported by the vendor?	Operating systems software, upgrades, and patches are up-to-date and supported by the vendor.		
19.	Are web server patches up-to-date and tested on non-production systems prior to implementation?	New patches are up-to-date and tested on non-production systems prior to implementation.		
20.	Are security patches applied in a timely manner?	All relevant security patches should be applied as soon as they have been validated through testing.		
21.	Are application development tools installed on the production web server?	Application development tools are not installed on the production web server.		
22.	Are change control and lifecycle management processes documented and implemented for the web farms?	Change control and lifecycle management processes are documented and implemented for the web farms.		
23.	Are security implications addressed for select components (i.e. programs, scripts, and plug-ins) of the web server?	Security implications have been addressed for select components of the web server. Consider security implications before selection of programs, scripts, and plug-ins for the Web server.		
24.	Is the Web server configured to minimize the functionality of programs, scripts, and plug-ins?	The web server has been configured to minimize the functionality of programs, scripts, and plug-ins.		
25.	Are scripts and other executables tested to ensure secure design?	Scripts and other executables are tested to ensure secure design. These scripts should be written with security in mind. They must be designed to handle user input in a secure manner.		

Step #	Procedure Description Web and FTP Server General Security	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
26.	Is the server configured to allow the execution of scripts and other executables only from a specific directory?	The server is configured to allow the execution of scripts and other executables only from a specific directory.		
27.	Are automatic directory listings disabled?	Automatic directory listings are disabled.		
28.	Is executable "Server Side Includes (SSI) disabled on the web server?	The "Server Site Includes" capability is disabled on the server. If the server must support executable SSI, SSI should be configured to turn off #exec includes by modifying the configuration files for the web server.		
29.	Are unnecessary files and "default" document trees removed or disabled?	Unnecessary files and "default" document trees have been removed or disabled. Remove ALL unnecessary files from the scripts directory and the /cgi-bin directory and all "default" document trees.		
30.	Are appropriate measures in place to identify, and control or remove vulnerabilities associated with the ability to query or display information from a database?	Appropriate measures are in place to identify, and control or remove vulnerabilities associated with the ability to query or display information from a database.		
31.	Is encryption used to transfer sensitive information over a Web connection?	Encryption is used to transfer sensitive information over a Web connection. Encryption should be enabled in order to transfer sensitive information over the Web connection (e.g., personal information).		
32.	Is file sharing not required for business purposes disabled on the system?	File sharing is disabled on the system. File sharing should be disabled. If files are shared on the network, require user authentication and set hard-to-crack passwords.		
33.	Is the number of OSs and web server versions minimized?	The number of OSs and web server versions is minimized. The number of OS and web server versions should be minimized. Every OS revision means a new set of vendor patches to keep track of, and a set of revisions and patches for all vendor installed. Limiting the number of operating systems and web server platforms leaves more time for securing each platform.		
34.	Are RPC (Remote Procedure Call) services that are not absolutely necessary removed?	You should eliminate any RPC services that are not necessary.		

Step #	Procedure Description Web and FTP Server General Security	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
35.	Are FTP servers located in the web farm protected from unauthorized access?	FTP servers located in the web farm are protected from unauthorized access.		
36.	Is anonymous access to FTP servers within the web farm restricted by specific ip domains or by a similar method?	Anonymous access to FTP servers within the web farm is restricted by specific ip domains or by a similar method.		
37.	Are separate upload and download directories implemented on FTP servers?	Separate upload and download directories have been implemented on FTP servers.		
38.	Is a process in place for approving uploaded files prior to their being made available for download?	A process is in place for approval of files prior to their being made available for download.		
39.	Are files placed in FTP upload directories tested for viruses, trojans and other malicious code prior to being made available for download?	Files placed in FTP upload directories are tested for viruses, trojans and other malicious code prior to being made available for download.		
40.	Are Unix FTP servers run in a chrooted part of the directory tree?	<p>Unix FTP servers are run in a chrooted part of the directory tree.</p> <p>Run the FTP server in a chrooted part of the directory tree so it cannot be used to access the real system files. The purpose of chrooting is designed to create a "jail" protecting what is being chrooted from being able to read or modify any files outside of the chrooted environment.</p>		

<p>Comments:</p>
<p>Action Plan:</p>

Test Number: 2	SYSTEM:	DATE:	TIME:
Test Name: Unix Based World Wide Web Server Security			
Resources Required:	Access to the Web Server(s).		
Personnel Required:	System Administrator or Web Server Administrator		
Objectives:	To determine that the Unix Based Web Servers are configured to meet USDA requirements pertaining to internet system protect, user access privileges, and network security.		
Procedure Description: (Summary)	Verify that access is properly controlled. Verify that the servers are run with as little privilege as necessary. Verify that server functionality is executed in a restricted file space. Verify that system integrity is monitored and maintained.		

Detailed Procedures and Results

Step #	Procedure Description Unix Based WWW Server Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
1.	Is the web server run in a chrooted part of the directory tree?	The web server is run in a chrooted part of the directory tree. Run the Web server in a chrooted part of the directory tree so it cannot access the real system files. The purpose of chrooting is designed to create a "jail" protecting what is being chrooted from being able to read or modify any files outside of the chrooted environment.		
2.	Is the web server run as user root?	The web server is not run as user root. The web server should not be run as user root. Set it to run as nobody user unique to the Web service.		
3.	Is the web server set to follow symbolic links?	The web server is not set to follow symbolic links. The server should not be set to follow symbolic links, or to only follow links that are owned by the same user that owns the destination of the link.		
4.	Is the Web server chrooted in a protected directory?	The Web server is chrooted in a protected directory.		

Step #	Procedure Description Unix Based WWW Server Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
5.	Is the best X11 authentication (e.g., Kerberos, Secure RPC, "magic cookies") enabled in the configuration instead of using xhost?	The best X11 authentication (e.g., Kerberos, Secure RPC, "magic cookies") is enabled in the configuration instead of using xhost.		
6.	Are netgroups/or groups used to restrict access to services?	Netgroups/or groups should be used to restrict access to services.		
7.	Does the portmapper perform proxy forwarding?	The portmapper should perform proxy forwarding.		
8.	If portmapper has a "securenets" feature, does it restrict which machines can send requests to the portmapper?	If portmapper has a "securenets" feature, it is configured to restrict which machines can send requests to the portmapper.		
9.	Is the server daemon run as a nonprivileged user (e.g., user "nobody") rather than as user "root"?	<p>The server daemon is run as a nonprivileged user (e.g., user "nobody") rather than as user "root".</p> <p>Most server daemons can be configured this way. Thus, if an intruder discovers a vulnerability in the server, he or she can only access files and executable programs with the privileges of a nonprivileged user.</p>		
10.	If a machine is administered remotely, is a secure shell used to make a secure connection?	<p>Remote administration is done via a secure shell connection.</p> <p>If the machine must be administered remotely, you should require that a secure capability such as secure shell be used to make a secure connection.</p> <p>Telnet or non-anonymous FTP (those requiring a username and password) connections to this machine from any untrusted site should not be allowed.</p>		

Comments:
Action Plan:

Test Number: 3	SYSTEM:	DATE:	TIME:
Test Name: Microsoft Internet Information Services Security Checklist			
Resources Required:	Access to the IIS 4 or 5 Server.		
Personnel Required:	Systems Administrator or Web Server Administrator		
Objectives:	To ensure that Microsoft's Internet Information Services (IIS) are securely configured.		
Procedure Description: (Summary)	Verify that the IIS server is properly configured and controlled. For information regarding Microsoft IIS, refer to: http://www.microsoft.com/windows2000/en/server/iis/		

Detailed Procedures and Results

Step #	Procedure Description Microsoft Internet Information Services Security Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
1.	For IIS 5 servers, is the Hisecweb.inf Security Template or similar template reviewed, updated, and deployed?	The Hisecweb.inf Security Template has been reviewed, updated, and deployed. Review, update, and deploy the provided Hisecweb.inf Security Template. Hisecweb.inf can be downloaded from: http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe		
2.	For IIS 5 servers, is the IPSec Policy configured or server level firewall deployed (i.e. IDS agent)?	The IPSec Policy is configured. TCP/IP protocols should be blocked with the exception of ports that are designated to be open. The IPSec administration tool or the IPSec Policy command line tool should be used to deploy the IPSec policy.		
3.	For IIS 5 servers is the Telnet Server disabled?	The Telnet Server is disabled. If the Telnet server included with Windows 2000 is utilized, access to this service should be restricted.		

Step #	Procedure Description Microsoft Internet Information Services Security Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
4.	Is NetBIOS disabled over TCP/IP?	<p>NetBIOS over TCP is disabled.</p> <p>To prevent attackers from executing NetBIOS Adapter Status command against a server and revealing through this command the name of the currently logged on user that could be maliciously used by attacker, disable NetBIOS over TCP on public connections of the server.</p> <p>Before disabling NetBIOS over TCP administrators need to ensure that it doesn't affect their management tools used to manage the server and other applications (if any) running on the server. For this purpose it is highly recommend disabling NetBIOS over TCP on a server in test environment before disabling it on the production servers.</p>		
5.	Is Remote Data Services (RDS) support, enabled by default, disabled?	<p>Remote Data Services (RDS) support is disabled.</p> <p>RDS capability should either be removed or usage should be restricted using ACLs. When incorrectly configured, RDS can make a server vulnerable to denial of service and arbitrary code execution attacks.</p>		
6.	Have the appropriate ACLs on virtual directories been set?	Appropriate ACLs on virtual directories have been set.		
7.	Is the W3C Extended Logging format being used for web services?	The W3C Extended Logging format is being used.		
8.	Have the appropriate IIS Log file ACLs been set?	<p>Appropriate IIS Log file ACLs have been set</p> <p>Make sure the ACLs on the IIS-generated log files (%systemroot%\system32\LogFiles) are Administrators (Full Control) System (Full Control) Everyone (RWC) This is to help prevent malicious users from deleting the files to cover their tracks.</p>		
9.	Where applicable have IP Address/DNS Address Restrictions been set on IIS 5 servers?	IP Address/DNS Address Restrictions have been set where applicable.		

Step #	Procedure Description Microsoft Internet Information Services Security Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
10.	Are Root CA Certificates on the IIS Server updated?	Root CA Certificates on the IIS Server are updated.		
11.	Have all sample applications been disabled or removed?	All sample applications have been disabled or removed. Samples should not be installed by default and should never be installed on a production server.		
12.	Are unneeded COM components disabled or removed?	Unneeded COM components are disabled or removed. Some COM components are not required for most applications and should be removed. Most notably, consider disabling the File System Object component, but note that this will also remove the Dictionary object. Be aware that some programs might require components you're disabling. Be sure to test the removal of COM objects on a non-production system first.		
13.	If the IIS server was upgraded from IIS 4 to IIS 5 has the iisadmpwd virtual directory been removed?	The iisadmpwd virtual directory has been removed. It is designed primarily for intranet scenarios and is not installed as part of IIS 5, but it is not removed when an IIS 4 server is upgraded to IIS 5. It should be removed if you don't use an intranet or if you connect the server to the Web.		
14.	Is <FORM> and Querystring Input in ASP Code checked?	<FORM> and Querystring Input in ASP Code has been checked. Many sites use input from a user to call other code or build SQL statements directly. In other words, they're treating the input as valid, well-formed, nonmalicious input. This should not be so; there are a number of attacks where user input is treated incorrectly as valid input and the user could gain access to the server or cause damage. Each <FORM> input and query string should be checked before passing it on to another process or method call that might use an external resource such as the file system or a database.		

Step #	Procedure Description Microsoft Internet Information Services Security Checklist	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
15.	Is the web server parent path disabled?	<p>Web server parent path is disabled.</p> <p>The web server parent path option allows you to use ".." in calls to functions such as <i>MapPath</i>. By default, this option is enabled, and you should disable it.</p>		

Comments:

Action Plan:

Acronyms

ADP	Automated Data Processing
DM	Data Manager
DR	Data Request or Data Requirement
FIPS	Federal Information Processing Standards
ISSPM	Information Systems Security Program Manager
OMB	Office of Management and Budget
SBU	Sensitive But Unclassified
USDA	United States Department of Agriculture