CHAPTER 7, PART 2
PATCH MANAGEMENT AND SYSTEMS UPDATES

1 BACKGROUND

USDA is among many federal agencies and private organizations that have been experiencing growing concern over the escalation in virus and worm activities. These types of activities jeopardize the operational availability, confidentiality and integrity of our Information Technology (IT) assets and impede accomplishment of our overall mission.

Failure to keep operating system and application software up to date is a common mistake made by information technology (IT) professionals. Despite extensive testing, all operating systems and applications are released with "bugs" (errors in the software) that affect security, performance, and stability. Most estimates for the number of bugs in published software range from 5 to 20 bugs per 1,000 lines of code.

Security-related bugs are generally discovered only after a large number of users start using the operating system or application and hackers or independent testers start attempting to expose and compromise vulnerabilities in the software. Once a bug is discovered, the software manufacturer often releases a piece of software to correct the bug. This software is often called a patch, hotfix, or service pack.

Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer or system. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also mitigate "unpatched" vulnerabilities through other methods (e.g. workarounds, firewalls, and router access control lists).

Today more than ever, a timely patch management response to vulnerabilities is critical to maintain the operational availability, confidentiality, and integrity of IT systems. Patches are usually released for three reasons:

a To fix faults in an application or operating system. Many hacker attacks are based on exploiting faults in the computer code of applications and operating systems. Patches are also released to correct performance or functionality problems.

b To alter functionality or to address a new security threat. An example of this is new virus definitions for an antivirus application. There was nothing "wrong" with the code of the antivirus program, but it had to be updated to detect new viruses that did not exist when the application was first released.

c To change or modify the software configuration to make it less susceptible to attacks and more secure.

CERT/Coordination Center (CC)3 (http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. In an increasingly interconnected world, it is critical that system administrators keep their systems patched to the most secure level. A common misperception among some system administrators is that a firewall reduces the need for timely patching. Unfortunately, this is incorrect because a firewall generally permits some level of traffic between most internal and external hosts. As long as a communication channel is allowed between the internal network and the Internet or other external network, there is a risk of compromise; thus patching becomes critical.

2 POLICY

All USDA agencies and staff offices will establish or implement an automated agency-wide system of patch management for all IT systems, devices and appliances, regardless of operating system or platform. This will consist of clearly assigned specific responsibilities for the System Administrator(s) or other authorized personnel. All authorized personnel must be trained in system administration to include patch management techniques. Patch management will be used in conjunction with the normal agency vulnerability scanning efforts. USDA agencies will use the department recommended tool or other approved automated patch management software. Agencies will certify that system patches have been applied using the USDA Monthly Patch Certification, Form A, included in this chapter. This certification form will be completed monthly by the agency ISSPM and sent with the Vulnerability Scan Certification.

Patches will be tested on non-production systems prior to installation on all production systems. In addition, each agency will create and maintain an organizational hardware and software inventory and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to external entities (DHS, GAO, OMB, etc) within constrained timeframes. CS reserves the right to review for compliance in patch management and vulnerability correction.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this policy exception as a Plan of Action & Milestone (POA&M) in their FISMA reporting until full compliance is achieved. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

Although the National Institute of Standards and Technology (NIST) recommends that agencies establish a "Patch and Vulnerability Group", this is optional in establishing a patch management program. Each agency should establish this program the most efficient and effective way possible given their need and the designation of a Patch Management Officer will be at the agency's discretion. At a minimum, the following duties and responsibilities will be delegated to the System Administrator(s) or other authorized personnel:

a Create and Maintain an Organizational Hardware and Software Inventory to include a Patch Management Database.
The System Administrator (SA) or other authorized personnel will create/maintain a database containing: the hardware equipment and software packages; version numbers of those packages within the organization; patches that apply to this equipment and patch status. Most automated patch management programs provide this capability and are preferred over manual patch solutions. This database should be directly linked to the baseline hardware/software inventory that is utilized in the agency Configuration Management (CM) Plan. This database will enable the SA or other authorized personnel to monitor for information about vulnerabilities and patches that correspond to the hardware and software within the inventory. Specific attention should be given to those software packages that are used on important servers or that are used by a large number of systems. This includes any government connected resources and any external resources

that are used for official USDA business. Once the organizational database has been created, it will be necessary to maintain this tool in a timely manner when a system is installed or upgraded. Post-patch distribution updates to the database/Configuration Management Plan will be executed immediately following any patching exercise.

b Identify Newly Discovered Vulnerabilities and Security Patches. The SA or other authorized personnel are responsible for proactively monitoring security sources for vulnerabilities and patches that correspond to the software within the organizational hardware and software inventory. A variety of sources should be monitored to ensure that they are aware of all the newly discovered vulnerabilities, including Security Alerts from CS.

When a vulnerability has no satisfactory patch, the SA will present alternative risk mitigation approaches to IT management and support the management decision by testing, documenting, and coordination implementation with the appropriate system or network administrators. Most automated solutions will perform the bulk of this requirement; any devices not covered by the automated system will be recorded manually in the database or Configuration Management Plan.

c Prioritize Patch Application The SA or other authorized personnel should be aware of the resource constraints of local administrators and should attempt to avoid overwhelming them (when possible) with a large number of patches. The SA or other authorized personnel must prioritize the set of known patches and provide advice to local administrators on the criticality of each patch. The criticality of a patch is a risk-based decision utilizing standard elements such as Probability and Consequence. In today's environment consideration of consequences usually extends beyond a system's logical boundaries and will require a broader approach in weighing this factor. Operating System (OS) Patches deemed critical by the software vendor will always be considered critical by USDA. A distinction must be made between servers and end-user systems when making patching recommendations because often it is more important to patch servers on a routine schedule before end-user systems and to more thoroughly patch the servers. Care should be taken to ensure that the automatic patch distribution solution targets the correct machines. Patches deemed critical will be tested and installed on applicable systems within calendar 14 days of general release. Engineering patches (patches not in general release) should be avoided unless the criticality is extremely high and the general availability release date poses a significant risk to the target systems.

d Conduct Testing of Patches based on priority

If an organization uses standardized host configurations, the SA or other authorized personnel will be able to test patches on non-production servers with those configurations. This will avoid the need for redundant testing by each local administrator. The SA or other authorized personnel should also work closely with local administrators to test patches on important servers systems.

e Distribute Patch and Vulnerability Information to Local Administrators

The SA or other authorized personnel are responsible for informing local administrators about patches that correspond to software packages included on the organizational software inventory. Email lists should provide an effective method for distributing patch information. However, to decrease the chance of a spoofed email containing a Trojan Horse patch, actual patches should be distributed from an internal secured server instead of from the emails themselves. Several email lists may be maintained that include administrators that are responsible for various types of systems (e.g., Unix versus Windows administrators).

f Verify Patch Installation Through Network and Host Vulnerability Scanning

The SA or other authorized personnel will probably not have the resources to verify that every patch has been installed on every machine unless a commercial Patch Management solution is implemented. Most automated patch software provides reports on patch installation and how they were applied to the target system. However, the SA or other authorized personnel should perform monthly network and host vulnerability scanning to identify systems that have not been patched as required by Chapter 6, Part 2, USDA Vulnerability Scan Procedures. Many commercial patching packages provide a linkage or seamless integration with existing vulnerability scanners. Whenever possible, patch management vulnerability scanning and configuration management should be tightly integrated. Immediate Scans are required for critical system patches. Scanning results will provide the SA or other authorized personnel with another data source for new vulnerabilities and patches. However, agencies should be aware that network and host vulnerability scanners do not check for every known vulnerability and thus cannot be relied on as a sole source of vulnerability information. The SA or other authorized personnel should inform local administrators that they are performing such monthly or immediate scanning because it will make the administrators more accountable to install each patch. NIST Special Publication 800-42, Guidelines on Network Security Testing, offers advice on techniques for vulnerability scanning.

g Identify Patches and Vulnerabilities Associated with Software On Local Systems

As previously mentioned, the organizational software inventory and patch database may not contain all software used by a local agency. Patches and vulnerabilities that cannot be updated using the automated patch management solution should be documented on an exception report and corrected. Most automated patch packages will permit agencies to build a custom package to deploy packages for in-house software applications and have the capability to provide a post-implementation snapshot for reporting patching levels throughout the target infrastructure. These snapshots should be an important part of the system's configuration management plan and be easily incorporated into any consolidated reporting to the department or other stakeholders. All patches applied or vulnerabilities identified will require correction and testing in accordance with the procedures outlined above.

4 RESPONSIBILITIES

a The Chief Information Officer/Deputy will:

Support the establishment of departmental patch management policy and procedures within USDA; ensure that funding and personnel are provided to effectively maintain enterprise-wide patch management solutions.

b The Associate CIO for Cyber Security will:

(1) Develop and publish policy and procedural guidance on patch management;

(2) Provide enterprise-wide tools to assist agencies in compliance efforts;

(3) Monitor patch management by agencies on a department-wide basis;

(4) Provide advice and guidance to agencies in effectively patching systems and eliminating vulnerabilities;

c The Associate CIO for Information Resources Management (IRM) will:

(1) Support exception requests from the patch management policy and procedures contained in this chapter to ensure that appropriate security protection is provided; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security.

d The Agency Chief Information Officer will:

(1) Establish and implement an internal agency program for patch management on all IT systems;

(2) Ensure that all IT professionals, especially System Administrators, Network Administrators and Information Systems Security Program Managers, are trained and made aware of this policy and procedures;

(3) Clearly assign system administrators and other authorized personnel specific patch management and vulnerability correction responsibilities;

(4) Employ the departmental or an approved automated patch management solution to facilitate compliance with this policy and to promote efficiency for all systems, wherever feasible; apply patch management solutions to in-house applications and monitor status of those systems;

(5) Ensure that an agency Inventory of Hardware and Software and Patch Status is developed in an electronic database to maintain and track status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements;

(6) Report patch management status monthly to OCIO using the Patch Management Certification Form and external organizations;

(7) Request a formal exception through the established process for any systems which are not compliant within 90 days.

e The agency Information System Security Program Managers/designated staff will:

(1) Become familiar with CS patch management policy, procedures, enterprise wide solutions and NIST SP 800-40;

(2) Ensure that all IT systems have System Administrators or other authorized personnel provide timely patch management to all agency systems;

(3) Act as a Point of Contact (POC) for security to provide guidance and assistance to the SA(s) or other individuals designated patch management responsibilities; and

(4) Complete the Patch Management Certification Form, Appendix A, for all agency systems.

-END-

Appendix A
USDA Monthly Patch Management Certification

Agency___________________________________ ISSPM Name_____________________________________

1. Number of Devices Patched in the Past 30 Days____________________________

2. Do these devices include all systems and desktops? Yes_________ No____________

2a. If no, please include an explanation to include target dates when all systems and desktops will be patched.

b. For systems not patched, have vulnerabilities been mitigated? Yes ____ No ____

If no, explain

3. If not, have Plan of Action and Milestones (POA&M) been created and reported under the Federal Information Security Management Act (FISMA) to address these unpatched systems? Yes__________ No_____________

Certification Signature:

______________________ ____________________________

Name **Date**