



Security Patch Management References In Government Regulation Documents

- **Appendix III to OMB Circular No. A-130 Security of Federal Automated Information Resources**
- **Department of Education Information Technology Security C&A Program Overview**
- **NIST 800-40 Procedures For Handling Security Patches**
- **NIST 800-61 Computer Security Incident Handling Guide**
- **ED System Security Plan Template**
- **FISMA**
- **MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
SUBJECT: Reporting Instructions for the Federal Information Security Management Act
and Updated Guidance on Quarterly IT Security Reporting**
- **ED Security Policy Handbook**
- **NIST Self-Assessment Guide 800-26**
- **FSA Information Technology Security and Privacy Policy (ITSP)**
- **FSA Security Incident Implementation Guide**

Department of Education's Handbook for Information Technology Security Policy (2.3.13 p. 9)

IT configuration management controls must include mandatory installation, verification and management of software patches and fixes on all Department servers, workstations and laptops within 30 days of release, or sooner, as security issues dictate.

NIST Self Assessment Guide

Appendix A - System Questionnaire

10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?

14.2.1 Is incident information and common vulnerabilities or threats shared with system owners of interconnected systems

Appendix C - Federal IT Security Framework Level 4

5.2.b Mechanisms for identifying vulnerabilities revealed by security incidents or security alerts - ...In addition they should review security alerts issued by FedCIRC, vendors, and others

5.2.c Process for reporting significant security weaknesses and ensuring effective remedial action. - Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.

August 6, 2003

M-03-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten Director

**SUBJECT: Reporting Instructions for the Federal Information Security Management Act
and Updated Guidance on Quarterly IT Security Reporting**

C. System configuration requirements determined by the agency

FISMA (section 3544(b)(2)(D)(iii)) requires that each agency develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and



Security Patch Management References In Government Regulation Documents

maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance

Additionally, while many agencies have established patch authentication and distribution accounts through FedCIRC's government-wide patch management contract, actual usage of those accounts are extremely low. To ensure that agencies maintain up-to-date patches, it is critical that usage increase.

D. Annual testing and evaluation of security controls

The necessary depth and breadth of an annual FISMA review depends on several factors such as: 1) the acceptable level of risk and magnitude of harm to the system or information; 2) the extent to which system configurations and settings are documented and continuously monitored; **3) the extent to which patch management is employed for the system;** 4) the relative comprehensiveness of the most recent past review; and 5) the vintage of the most recent in-depth testing and evaluation as part of system certification and final accreditation.

For example, if in the previous year a system underwent a complete certification and received final (not interim) authority to operate, has documented configuration settings, employs automated scanning tools to monitor configurations, threats, and vulnerabilities, and has an effective patch management capability, a simple maintenance review using NIST's self assessment tool may meet the FISMA annual review requirement. If none or only some of the foregoing are true, then the annual testing and evaluation must be far more comprehensive commensurate with the acceptable level of risk and magnitude of harm. Agency officials must use sound judgment when determining the scope and rigor of FISMA's annual test and evaluations.

Questionnaire in memo included:

How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?

Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?

If yes, how many active users does the agency have for this service?

Has the agency developed and complied with specific configuration requirements that meet their own needs?

Do these configuration requirements address patching of security vulnerabilities?

Appendix III to OMB Circular No. A-130 Security of Federal Automated Information Resources

B.3.a.3 Review of Security Controls.

Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches^{*†}), and penetration testing can assist in the on-going review of different facets of systems.

NIST 800-40 Executive Summary Recommends:

Having an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.

One of several possible techniques is through the creation of a patch and vulnerability group (PVG). This group would facilitate the identification and distribution of patches within the organization. Its duties should include:

1. Creating an organizational hardware and software inventory^{*†}



Security Patch Management References In Government Regulation Documents

2. Identifying newly discovered vulnerabilities and security patches*†
3. Prioritizing patch application
4. Creating an organization-specific patch database*†
5. Testing patches for functionality and security (to the degree that resources allow) *†
6. Distributing patch and vulnerability information to local administrators
7. Verifying patch installation through network and host vulnerability scanning*†
8. Training system administrators in the use of vulnerability databases
9. Deploying patches automatically (when applicable) *†
10. Configure Automatic Update of Applications (when applicable). *†

If organizations use the PVG approach, this would not diminish the responsibility of all systems administrators to patch the systems under their control. Each systems administrator would:

1. Apply patches identified by the PVG
2. Test patches on the specific target systems
3. Identify patches and vulnerabilities associated with software not monitored by the PVG

Besides creating a PVG, organizations should be aware that applying patches and mitigating vulnerabilities is not always a straightforward process.

NIST 800-61 2.5 Incident Response Team Services

Patch Management *Giving the incident response team the responsibility for patch management (e.g., acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization) is **generally not recommended**. Patch management is a time-intensive, challenging task* that cannot be delayed every time an incident needs to be handled. In fact, patch management services are often needed most when attempting to contain, eradicate, and recover from large-scale incidents. Effective communication channels between the patch management staff † and the incident response team are likely to improve the success of a patch management program.*

NIST 800-61 3.12 Preventing Incidents

Patch Management. Many information security experts agree that a large percentage of incidents involve exploitation of a relatively small number of vulnerabilities in systems and applications. Large organizations should implement a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches. *†

NIST 800-61 4.4.1 Choosing a Containment Strategy

Correct the Vulnerability or Weakness That Is Being Exploited

If an unpatched operating system is susceptible to a DoS from specially crafted packets, patch the operating system.

Department of Education Information Technology Security C&A Program Overview

Configuration Management Plan (CMP)

A CMP maintains control of a system throughout its life cycle by ensuring that change control is appropriately applied and that proper security controls are consistently implemented. *† The CMP validates that changes take place in a controlled environment, and that the changes do not adversely affect the system.

FSA ITSP 3.7 Configuration Management

Every FSA System Manager must create a configuration management plan that describes the *hardware and software maintenance controls* in place and the process by which configuration controls will be maintained for that system.



Security Patch Management References In Government Regulation Documents

FSA ITSPP 3.7.2.1 Maintenance and Repair

FSA System Managers must implement access controls and *other security precautions to prevent potentially malicious code, such as “back doors”*, from being used to evade authentication and authorization protections

System Managers must periodically must review their systems for *known vulnerabilities and current installation of software patches*. These reviews are separate from the C&A review conducted by the DAA.

FSA ITSPP 3.7.2.2 Unapproved Software

The department must perform periodic audits of FSA computers to make sure *users do not install unapproved software*. *

FSA ITSPP 3.8 Incident Response

The confidentiality, integrity, and availability of FSA networked systems will depend in part on the preventative security measures to deter or inhibit attacks.

FSA ITSPP 3.8.1 Information Sharing

FSA must share information regarding incidents and common vulnerabilities or threats with FSA system personnel and appropriate managers of systems and networks interconnected with FSA and with the department level security office. *†

FSA System Security Plan Template Security Patches

All EDNet security remediation resulting in patches or upgrades to OEF systems will be under the following conditions—

- Performed by EDNet staff.
- OEF staff will be notified prior to any work via EDNet Tech Notice.
- The prioritization of work associated with patching to correct a security related vulnerability is a factor of the amount of risk associated with the vulnerability. The amount of risk is assessed by considering the following factors:

Whether EDNet assets manifest the vulnerability

The amount of loss that would be sustained if the vulnerability were exploited

Whether those assets that manifest the vulnerability are exposed to impending attack.

Accordingly, the following work prioritization is applied when a vendor announces a security related patch:

For high-risk security patches: The importance attached to deployment of a patch that corrects a high-risk vulnerability (as categorized by the Operational Security Review Committee) is second only to responding to an incident. Therefore the acquisition, testing, and deployment (assuming that the results of testing are satisfactory) of the patch are performed immediately.

For medium risk security patches (as categorized by the Operational Security Review Committee) the acquisition, testing, and deployment (assuming that the results of testing are satisfactory) of the patch is performed within 7-10 days.

For low risk security patches (as categorized by the Operational Security Review Committee) the acquisition, testing, and deployment (assuming that the results of testing are satisfactory) of the patch is performed at the next quarterly patch evolution.



Security Patch Management References In Government Regulation Documents

Items of Responsibility: EDNet Routine Operational Tasks

OS updates/patches	OCIO Operations is responsible for applying all patches. OCIO Operations will notify the OEF system technical leads of what patches are being applied, what for, and when they will be applied as needed.
--------------------	---

From NIST Computer Incident Handling Guide

Appendix B.2 Scenarios

Scenario 3: Worm and DDoS Agent Infestation On a Tuesday morning, a new worm is released on the Internet. The worm exploits a Microsoft Windows vulnerability that was publicly announced 2 weeks before, at which time patches were released. The worm spreads itself through two methods: (1) e-mailing itself to all addresses that it can locate on an infected host and (2) identifying and sending itself to hosts with open Windows shares. The worm is designed to generate a different attachment name for each copy that it mails; each attachment has a randomly generated filename that uses one of over a dozen file extensions. The worm also chooses from more than 100 e-mail subjects and a similar number of e-mail bodies. When the worm infects a host, it gains administrative rights and attempts to download a distributed denial of service (DDoS) agent from different IP addresses using File Transfer Protocol (FTP). (The number of IP addresses providing the agent is unknown.) Although the antivirus vendors quickly post warnings about the worm, it spreads very rapidly, before any of the vendors have released signatures. The organization has already incurred widespread infections before antivirus signatures become available 3 hours after the worm started to spread. The following are additional questions for this scenario:

1. How would the incident response team identify all infected hosts?
2. How would the organization attempt
3. How would the organization attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?
4. Would the organization attempt to patch all vulnerable machines? If so, how would this be done?
5. How would the handling of this incident change if infected hosts that had received the DDoS agent had been configured to attack another organization's Web site the next morning?
6. How would the incident response team keep the organization's users informed about the status of the incident? What if e-mail services were overloaded or unavailable due to the worm?

What additional measures, if any, would the team use to take care of hosts that are not currently connected to the network (e.g., staff members on vacation, offsite employees who dial in occasional

FSA Security Incident Implementation Guide

2.0 INCIDENT PREVENTION

“An ounce of prevention is worth a pound of cure” is an old saying, but one that is particularly true for IT infrastructure. Practical experience has proven that the large majority of computer incidents can be avoided by taking small, appropriate, and timely measures. All FSA systems are required to prevent incidents by deploying proven software and devices, including anti-virus products, intrusion detection systems and devices, firewalls, IT security awareness training, and patch management tools and techniques. Section 3.8 of FSA's Information Technology Security and Privacy Policy (FSA Security Policy), Incident Response, also underlines the need for preventative security. However, all preventative measures and devices will be effective *only* if 1) the system uses appropriate security measures – devices or software - according to its use and needs and 2) the software and devices are properly updated, patched, and configured.



Security Patch Management References In Government Regulation Documents

Patch management techniques and tools are therefore essential to incident prevention. On the one hand, properly deployed and patched/updated software or hardware is difficult to compromise. On the other hand, improperly or unpatched/nonupdated items are the primary reasons for a security incident. The following section discusses the patch and update management considerations at FSA

2.1 Patch and Update Management

Patch management is only one component of security management in general, as the confidentiality, integrity, and availability of FSA systems depends in large part on the preventative security measures taken to deter or inhibit attacks. More specifically, patch management is a subset of configuration and change management processes. As mentioned above, patch management is also closely linked to incident response.

Section 3.7 of the (FSA Security Policy) specifically addresses configuration/change management. Further, all FSA systems have configuration management plans that adhere to the Departmentwide configuration management guide.

In addition to rapidly report on system coverage, FSA is increasingly being required to also report on the level of each system's specific patch and update coverage. This suggests the need for automated patch management tools, which can easily and quickly supply such information for large networks.

To help meet current Federal requirements, FSA has established an email alert process that informs system personnel of new security fixes, patches, and problems. It has also established a process for tracking and reporting implementation compliance for patches and fixes.

2.2 Procedures for IT Security Alerts

The FSA Security and Privacy Team (S&P Team) issues two categories of IT security alerts -- low-to-medium-level threats and high-level threats (these are also identified as critical alerts). Each category requires action by an FSA contractor and/or the system's System Security Officer (SSO). Although the low-to-medium alerts are of interest and require appropriate action, these actions can usually be scheduled so they do not interfere with normal business operations. On the other hand, high-level, or critical alerts need immediate action to prevent an imminent security incident that could deny access, release private citizens' data, damage the Department's reputation, or incur major expenses for reconstitution of the system.

2.2.1 Low-to-Medium Alerts

The FSA S&P Team regularly forwards IT security alerts to the SSOs for all FSA systems. These alerts are routinely disseminated on Tuesdays and Fridays, and normally contain a mixture of low- and medium-level vulnerabilities. When the routine Tuesday and Friday alerts are issued, SSOs are expected to pass the information on to the technical support staff for the system, be it a government employee or contractor employee. Together with such staff, the SSO will determine which of the alerts indicates a risk to their system, and take appropriate action to prevent the threat or attack from affecting the system. There is no requirement to report on the status of any given threat/vulnerability/remediation effort, though the SSO should be ready to respond to inquiries concerning an alert.

2.2.2 Critical Alerts

When a high-level, or critical alert is issued by FedCIRC, OMB, a manufacturer, or another source, the FSA S&P Team will *immediately* issue the alert to both the appropriate SSOs and contractor contacts. For systems residing at the Virtual Data Center (VDC), CSC staff (the contractors who run the VDC) will be notified, along with the VDC SSO. The SSO and contractor contacts for systems with components external



Security Patch Management References In Government Regulation Documents

to the VDC will also be notified. A list of contacts for the alerts is maintained by the FSA CSO. SSOs should check with the CSO to update the contact information for their systems. Periodically, the list will be disseminated for updating, but changes to the contact list should be forwarded to the S&P Team as soon as they are applicable.

- High-level or critical alerts will be issued by email (first line of alert) and by telephone (second line for follow up, and when an email acknowledgement has not been provided). When an alert requires immediate action, the email message will bear a specific title, such as that shown below:
 - **Special Threat Alert & Response (STAR) – Immediate Action Required**
 - The opening paragraph of the alert will provide a description of the special action needed as well as a reminder of the contact information for people in the S&P Team. Technical details of the alert will be included in the email message, either as text or as a file attachment.
- When a “**STAR**” alert is issued, the “owners” of the IT systems to which the alert is directed are responsible for reporting the status of remediation efforts. This reporting can be done by either the SSO or the contractor contact. In either case, the other party must be included as a cc: for the message.
- An FSA reporting form identifying the number of affected components, the number of fixes, and dates, along with other pertinent information, will be included with each new STAR alert. If there are special reporting formats required by OMB, ED CIO, or other government agency with oversight responsibility, they also will be provided with the alert.
- A report must be filed within 2 hours of receipt of the alert. The report should be sent to the S&P Team member who sent the alert. The initial report can be a simple acknowledgement that the alert was received. Remediation decisions, installation of system patches or work-arounds, and other pertinent status information will be conveyed in timely followup reports. Upon occasion, government agencies or offices with oversight responsibility may request reports within a shorter time period.
- In any case, reporting and remediation of critical vulnerabilities will be given high priority by the system owner and system manager, and any decision to delay actual remediation (by using work-arounds) must be agreed to by the system manager. If sound business reasons exist to delay applying a patch or installing an upgrade that could/would remediate the threat/vulnerability, the system manager must state in writing the reason for the delay and must obtain concurrence of the FSA CIO.
- When a work-around is used in place of full remediation, the status for that system will be kept “open” until remediation is accomplished. Both ongoing remediations as well as a final report should be filed once full remediation is accomplished.

2.3 Tracking

The FSA S&P Team will maintain a data system that allows the status of each critical vulnerability to be tracked for each system.