



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-02-06-2013

DIVISION OF INFORMATION TECHNOLOGY

Patch Management Standard

Date of Last Revision 03/17/2013

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Purpose

- a. Security and other vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal business operations in addition to placing the State's data at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security or operating system vulnerabilities. Given the large number of computer workstations and servers that comprise the State's enterprise network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute these patches automatically when they are made available. The patch management solution has the ability to evaluate individual computer workstations and servers for vulnerabilities. Patches may then be automatically installed and, when necessary, the affected machine rebooted. Effective security is a team effort involving the participation and support of every state employee and affiliate who is a user of the State's enterprise network.
- b. The Division of Information Technology (DoIT) shall govern the implementation and operation of a Patch Management system on the State's enterprise network.

2. Definitions

- a. **The Microsoft Windows Server Update Services (WSUS)** - enables information technology administrators to deploy the latest Microsoft product updates to computers running Microsoft windows Server 2003, Microsoft Windows® XP with Service Pack 1, and Windows 2000 with Service Pack 4 operating systems. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network. The WSUS server provides the features that administrators need to manage and distribute updates through the WSUS Administration Console, which can be installed and accessed on any Windows computer in the domain. It works by controlling the Automatic Updates applet already present on all Windows machines. Instead of many machines all going to Microsoft's website to download updates, the WSUS server downloads all updates to a DOIT owned server and workstations on the domain look for updates.
- b. **Patch Management Group** – The Functional Group that has been delegated the authority to control patch releases.

3. Scope

- a. This standard applies to any Agency's implementation of Active Directory™. This standard covers implementation of any Server or Workstation established within Active Directory™ on the State's enterprise network within a production environment.

4. Standard

- a. Department, agencies, boards and commissions, and other entities participating in the State's Active Directory™ shall comply with the Patch Management prescribed standards, processes, and specifications defined by the Division of Information Technology. DoIT will publish specific procedures and processes that Agencies will follow to implement Active Directory™.

b. Control

- (i.) When a patch is released, the Patch Management Group will define the patches to be deployed to the State network. Patch deployment will be based on the level of criticality, existing infrastructure and treat assessment.

c. Patch Approval Process

- (i.) The Patch Management Group will decide whether or not the patch will be declared to be mandatory. Once a patch is declared to be mandatory, it will be tested by the supporting group. If the testing does not reveal serious compatibility problems, the mandatory patch will be approved for deployment.

d. Implementation

- (i.) The patch will be implemented by DoIT using the Microsoft Windows Server Update Services (WSUS). The DoIT implementation of Microsoft WSUS has two main components: one or more WSUS Update Servers and the Automatic Update Service. The WSUS Update Server is a supported Windows server running IIS and Update Server software from Microsoft. The Automatic Update Service runs on Windows 2003, Windows 2000 and Windows XP computers. The Automatic Update service on these computers in the RI.GOV domain and all other sub-domains will be configured using a group policy object (GPO). The WSUS GPO will automatically set several parameters; one of the parameters points the systems to the DoIT WSUS Update Server. Sometime after a the system is configured by the WSUS GPO, the set of patches installed on the system will be compared with the set of mandatory patches; any missing mandatory patches will be deployed.

5. Exceptions

- a. Requests for variance and exceptions to this standard must be submitted through the DoIT change management process.

6. Signatures

Assistant Director of Planning, Policy & Technology

Date

Director of Operations

Date

Chief Information Officer

Date

Director, Department of Administration

Date