Compliance Component

DEFINITION	
Name	Operation and Maintenance Phase (Security Patch Management)
Description	Operation and Maintenance Phase (Security Patch Management) of System Life Cycle Security is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an agency. Patches are additional pieces of code developed to enable additional functionality or address security flaws within a program. Flaws expose vulnerabilities that can be exploited by a malicious entity to gain unauthorized access.
Rationale	Security patch management will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred.
Benefits	• Reduce the resources utilized when dealing with vulnerabilities • Reduce the exploitation of vulnerabilities Note: "The Cost of an un-patched vulnerability can be as high as:" W * T * R, where (W) is the number of workstations, (T) is the time spent fixing systems or lost in productivity, and (R) is the hourly rate of the time spent. Example - For an agency where there are 1000 computers to be fixed, each taking an average of 8 hours of downtime (4 hours for one worker to rebuild a system, plus 4 hours the computer owner is without a computer to do work) at a rate of $70/hour for wages and benefits: 1000 computers * 8 hours * $70/hour = $560,000 to respond after an attack.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	System Life Cycle Security
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	A Patch and Vulnerability Group (PVG) should be created as a formal group that incorporates representatives from information security and operations. These representatives should include individuals with knowledge of vulnerability and patch management, as well as system

administration, intrusion detection, and firewall management. In addition, it is helpful to have specialists in the operating systems and applications most used within the agency. Personnel who already provide system or network administration functions, perform vulnerability scanning, or operate intrusion detection systems are also likely candidates for the PVG.

The duties of the PVG are outlined below.

1. Review System Inventory. The PVG should use an inventory of the agency's IT resources to determine which hardware equipment, operating systems, and software applications are used within the agency that should be patched.

2. Monitor Sources for Vulnerabilities, Remediation, and Threats. The PVG is responsible for monitoring security sources for vulnerability announcements, patch and non-patch remediation, and emerging threats that correspond to the software within the PVG's system inventory.

3. Prioritize Vulnerability Remediation. The PVG should prioritize the order in which the agency addresses vulnerability remediation.

4. Create an Agency-Specific Remediation Database. The PVG should create and maintain a database of remediation that needs to be applied to the agency.

5. Conduct Initial Testing of Remediation. The PVG should be able to test patches and non-patch remediation on IT devices that use standardized configurations. The PVG should also work closely with local administrators to test patches and configuration changes on unique systems.

6. Inform Local Administrators. The PVG is responsible for informing local administrators about vulnerabilities and remediation that will be distributed to software packages within the agency's software inventory.

7. Deployment of Patches. The PVG should deploy patches automatically to IT devices using enterprise patch management tools if available. Multiplatform environments, nonstandard systems, legacy systems, and systems with unusual configurations may need to be patched manually.

8. Automatic Update of Applications. Automatic application updates can be obtained from a locally distributed automated update process, where the patches are tested and made available from the agency's network. Applications can then be updated from the local network instead of from the Internet.

9. Verify Vulnerability Remediation. The PVG verifies that vulnerabilities have been successfully remediated through network and host vulnerability scanning.

	10. Vulnerability Remediation Training. The PVG and administrators should be trained on vulnerabilities and remediation. Note: Not all vulnerabilities are known or have related patches; thus, system administrators must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities. Note: End users should not have the permissions to apply patches.		
Document Source Reference #	NIST SP 800-40 Version 2		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	System Life Cycle, exploitation, bugs, vulnerabilities, malicious, remediation, maintenance, monitor, threats, holes, defects, bad code.		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		

AUDIT TRAIL			
Creation Date	09-07-06	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			