SMG 3210.8

FDA Staff Manual Guides, Volume III – General Administration

Information Resources Management

Information Technology Management

Patch Management Policy

Effective Date: 04/30/2024

1. Purpose.

This Staff Manual Guide outlines the roles and responsibilities ensuring the effective and timely application of patches. This policy will strengthen the Food and Drug Administration's (FDA) ability to effectively protect our network, systems, and sensitive data against vulnerabilities that could impact FDA operations.

2. Background.

Cyber threats, vulnerabilities, and risks to the FDA's IT infrastructure, systems, and applications are on the rise. External and internal threats are leveraging software flaws and computer access to exploit sensitive information and/or negatively impact the FDA mission and U.S. national and economic security. Potential threats and dangers due to not installing patch updates can include damaged software, loss of sensitive information, and system availability. Patch management is the process to identify, acquire, test, install software and configuration updates (patches), and verify that the patches were installed for FDA hardware, software, and networks.

In accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40 *Guide to Enterprise Patch Management Technologies*, Patch Management is required by various security compliance frameworks, mandates, and policies to maximize protection against IT security and privacy vulnerabilities. Additionally, NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations* requires installation of security- relevant software and firmware patches, testing patches before installation, and

incorporating patches into the organization's configuration management processes.

3. Policy.

The policy describes requirements to effectively apply patches in a timely manner to mitigate vulnerabilities. The System Owners of FDA information systems and networks must ensure that System Managers:

A. Use the NIST Common Vulnerability Scoring System (CVSS) summarized in the table below and ensure patches are complete on FDA information systems and networks within the required timeframes.[1]

Patch Risk Level	CVSS Base Score	Patch Implementation Required
Critical	9.0 - 10	15 Days
High	7.0 - 8.9	30 Days
Medium	4.0 - 6.9	30 Days
Low	0 - 3.9	60 days

B. Prioritize and implement normal cycle patches based on the risk level on FDA systems and networks in a manner that ensures maximum protection against IT security and privacy vulnerabilities and minimizes the impact on FDA business operations.

C. Apply emergency and out of cycle patches needed to resolve an exploit or vulnerability within 48 hours, at the direction of the Chief Information Security Officer (CISO).

D. Contribute to a centralized patch repository with historical views and patch back-out procedures.

E. Integrate patch management with change management.

F. Test and validate the integrity of patches before installation to avoid operational disruptions and ensure they are appropriately implemented on the system.

G. Submit a plan to apply the patch in a less than one year timeframe for consideration of an approved waiver from the FDA CISO if a security patch is not applied. Note that exceptions to patches are not permanent.

---

[1] Patch risk levels are determined by the vendor based on the National Institute of Standards and Technology (NIST) Common Vulnerability Scoring System (CVSS). Vulnerabilities with a CVSS base score in the range 7.0-10.0 are Critical/High, those in the range 4.0-6.9 are Medium, and 0-3.9 are Low.

4. Responsibilities.

A. **FDA Chief Information Officer (CIO)**. The CIO has the overall responsibility to manage the Agency IT security program.

B. **FDA Chief Information Security Officer (CISO)**. The CISO, appointed by the CIO, directs and oversees the FDA IT security program. The CISO is responsible for developing procedures, standards, and guidance, as well as for providing advice and assistance.

C. **System Owner (SO)**. The SO is responsible for coordinating all facets of the system's lifecycle, from design through implementation and maintenance. SO's are ultimately responsible for ensuring that System Managers are adhering to all security patch management policies and guidelines.

D. **System Managers**. System Managers are responsible for the operation and maintenance of enterprise patching systems. This includes testing patches, recommending application of tested patches, monitoring the successful completion of the deployment of patches, and validating that patches have been applied and correctly implemented.

E. **Users**. Anyone requesting and receiving approval to use hardware or software through the Technology/Product Request process or Enterprise Performance Life Cycle (EPLC) process is responsible and shall follow the above policy requirements to implement patching.

5. Procedures.

This policy document governs the patch policy procedures. Refer to the patching procedures for systems in the appropriate FDA repositories.

6. References.

HHS-OCIO Policy for Information Security and Privacy Protection, November 2021

HHS Policy for Personal Use of Information Technology Resources, HHS-OCIO- 2013-0004, August 1, 2013

NIST NVD Common Vulnerability Scoring System Support, Version 2.0

NIST Special Publication 800-40 Rev 4, Guide to Enterprise Patch Management Technologies, April 2022

NIST Special Publication (SP) 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

Federal Information Security Modernization Act (FISMA) of 2014, Public Law 107-347

7. Effective Date.

The effective date of this guide is April 30, 2024.

8. Document History – SMG 3210.8, "Patch Management Policy"

Status (I, R, C)	Date Approved	Location of Change History	Contact	Approving Official
Initial	01/07/2015	N/A	FDA Chief Information Security Officer	Walter Harris, FDA Chief Operating Officer
Revision	07/01/2020	N/A	FDA Chief Information Security Officer	Amy P. Abernethy, FDA Chief Information Officer
Revision	04/30/2024	N/A	FDA Chief Information Security Officer	FDA Chief Information Officer