To understand the current patching expectations for government assets and ISB expected patch mitigation plan for vulnerable systems based on risk rating

OCIO Patch Guidelines

Vulnerability and Risk Management

Risk Rating	Examples *(*If criteria is met apply patches as required)*	CVSS Score	ISB Patching Recommendation
CRITICAL	Vulnerability allows remote code execution Critical business system/information affected Exploits exist and are in use System is connected to the Internet without having mitigating controls in place	**9.8 - 10**	**Within 72 Hours** **Formal acceptance of risk is required for <u>all</u> instances in which patching cannot be completed during the recommended time frame.*
HIGH	Vulnerability allows remote code execution Essential business system information affected Proof of Concepts exist and are in use The system is in a protected enclave with strong access controls	**7.0 – 9.7**	**Within 14 Calendar Days** **Formal acceptance of risk is required for <u>all</u> instances in which patching cannot be completed during the recommended time frame.*
MEDIUM	Vulnerability allows an attacker with access to impersonate a legitimate user System is exposed to unauthenticated users System requires two-factor authentication and administrator-level remote login is disallowed	**4.0 – 6.9**	**Within 30 Calendar Days** *(if updates available)* Or at the next update, or within 3 months (i.e. Oracle or other vendors on a quarterly patch schedule) whichever is sooner.
LOW	A vulnerability requires authenticated users to perform malicious actions, such as SQL injection Affected system contains non-sensitive, publicly-available information Mitigating controls exist that make exploitation unlikely or very difficult	**0.1-3.9**	**Within 1 Year** Or at the next major update which ever is sooner.