CHAPTER 4: VULNERABILITY REMEDIATION/MITIGATION

4.1 VULNERABILITY REMEDIATION/MITIGATION INTRODUCTION

4.1.1 The goal of the vulnerability remediation/mitigation process is to mitigate risk to the AFIN through the implementation of network vulnerability countermeasures. Countermeasures will generally entail configuration changes to systems, installation of software patches, and/or the search for and removal of specific files or tools used for malicious purposes.

4.2 VULNERABILITY REMEDIATION/MITIGATION GENERAL PROCEDURES

4.2.1 Vulnerabilities will be remediated (e.g., patched) according to the applicable network order and associated timelines (Ref. Chapter 2).

4.2.2 Vulnerabilities will be remediated according to the direction provided through the applicable vulnerability management order. Severity of the vulnerability and risk associated to the network will drive the compliance timeframes.

4.2.3 The NOS/299 NOSS (ANG) are responsible for patching vulnerabilities on servers, network infrastructure, boundary devices and all other IP capable assets within their respective AOR utilizing both enterprise automated tools and manual processes

4.2.3.1 NOSs will implement a goal of 95% compliance of vulnerability remediation actions using enterprise remediation tools (e.g., SCCM, Automated Remediation and Asset Discovery (ARAD), etc.).

4.2.4 The base CFPs are responsible for monitoring client health and assisting the NOSs with remediation of vulnerabilities that cannot be remediated with enterprise automated tools.

4.2.4.1 Bases will alert NOS/COSs through appropriate incident response methods when non-clienteed machines rise above 10% and will cross-reference ACAS DNA with Active Directory and SCCM clienteed machines to obtain a more accurate number of systems.

4.2.4.2 Once the 95% threshold is met by the NOS/COSs, remediation of remaining assets and/or enterprise remediation clients (e.g., SCCM, ARAD, etc.) are the responsibility of the local base, PMO administrators or other responsible entity.

4.2.4.3 Compliance percentages shall be verified via vulnerability scans provided by network VATs responsible for the applicable assets (i.e., local base, PMO administrators, etc.).

4.2.5 The CFPs/NCCs will be responsible for identifying the information systems controlled by a PMO within their respective AOR. PMO systems will be patched only upon approval of the PMO or system owner (Ref. Section 4.9).

4.2.5.1 Only registered/approved programs within Enterprise Mission Assurance Support Service (eMASS) where an Interim Approval to Operate/Approval to Operate/Connect (IATO/ATO/ATC) through the DOD Risk Management Framework (RMF) process has been granted are considered PMO systems. For additional information on the RMF and eMASS program see the following links:

4.2.5.1.1 DODI 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP) – (http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf)

4.2.5.1.2 Enterprise Mission Assurance Support Service (eMASS) – (https://emass-airforce.csd.disa.mil/)

4.2.6 Base NCCs/CFPs are required to populate NOS patch testing groups with at least 3% of the base's total assets that includes a representative sample of every configuration at the base and systems from each mission set.

NOTE

NCC/CFP will review test groups biannually to ensure bases are meeting the 3% requirement. This will be verified periodically by the NOS . If testing groups do not meet the 3% requirement, systems will be selected at random by the NOS and added to the correct security group. The security groups within Active Directory used for identifying a test system are named using the following format: BASENAME_TEST_GROUP.

4.2.7 Base NCCs/CFPs will notify the servicing NOS of issues arising from the testing of automated patches by opening a ticket in the applicable trouble ticketing system (currently Remedy).

4.3 FIGURE 4-1 IS A GRAPHIC ILLUSTRATION OF THE MONTHLY VULNERABILITY REMEDIATION PROCESS. THE FLOW CHART DEMONSTRATES THE PROCESSES FOR NOS-LEVEL FUNCTIONS.

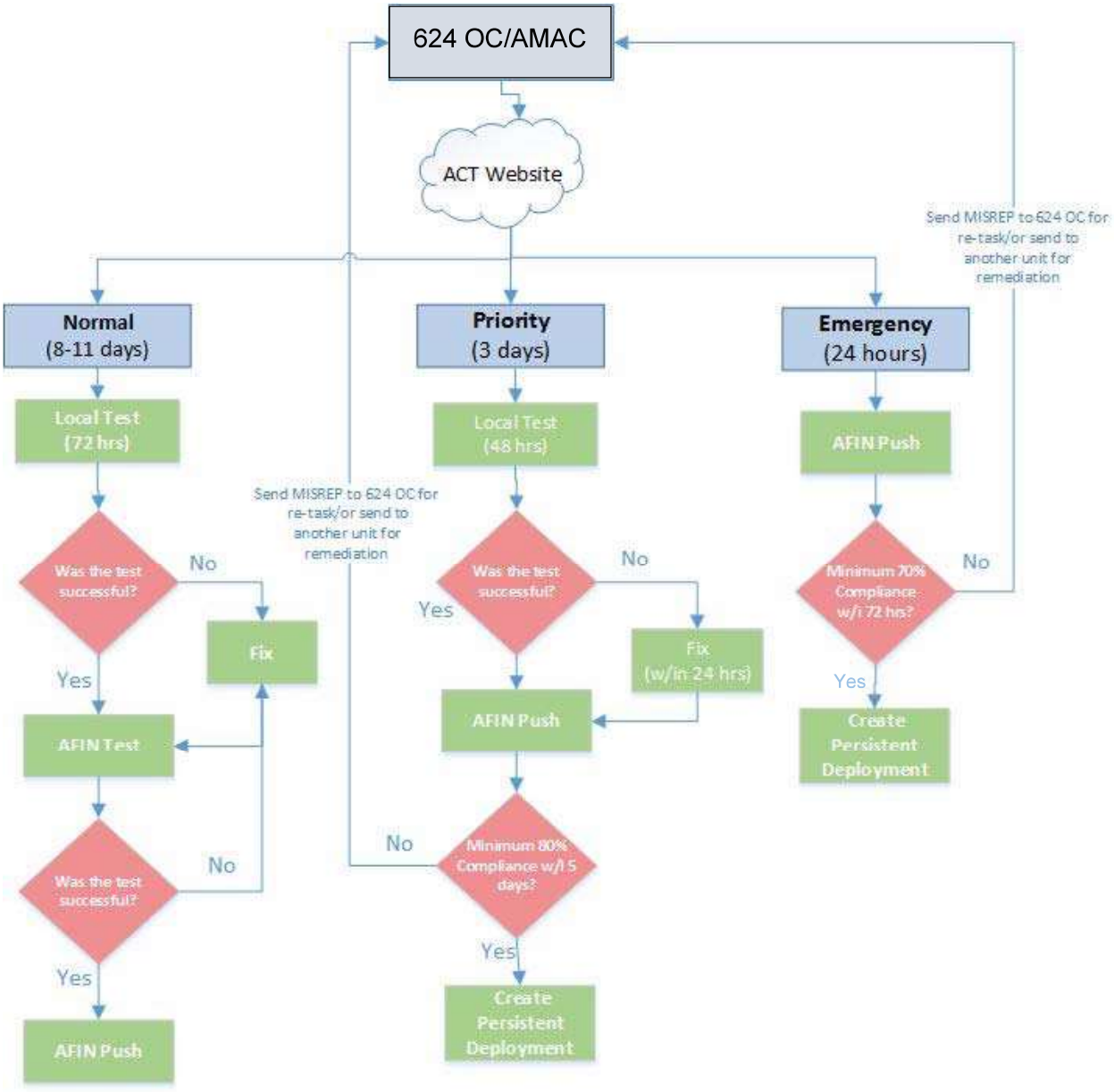

Figure 4-1. Three-Tiered Prioritization Model

4.3.1.1 **Normal (11 days)**: Vulnerability Remediation Operators (VRO) at the NOS will implement a two-phased patch testing approach. VROs will first issue patches to a local testing environment for up to 48 hours to ensure any issues that may be discovered shall have insignificant impact to the AFIN. If issues are discovered, VRO personnel will report these issues to the responsible party per the issued order. If no issues are discovered, VROs will issue patches to the AFIN 3% Test Group for a period of at least 3 days not exceeding 5 days. If issues are discovered, VRO personnel will report these issues to the responsible party per the issued order. If no significant issues are discovered, VRO

personnel will issue patches AFIN-wide in a persistent manner until the applicable orders are rescinded or the patch is superseded (significance will be determined by the CSCS functional lead for Vulnerability Management).

4.3.1.2 **Priority (3 days)**: VRO Patch Management technicians will test patch for 48 hours. Once successfully tested, VRO Patch Management Team will have 24 hours to deploy to enterprise, with mandated minimum 80% compliance of machines with remediation clients installed after 5 days of enterprise release. If minimum compliance is not met, VRO Crew will report back to 624 OC through Mission Report (MISREP) for action to re-task or send to another unit for remediation. If compliance of 80% or greater is reached, then a persistent deployment will be created.

4.3.1.3 **Emergency (24 hours)**: VROs will forgo all testing. Upon notification to VRO Crew Commander (CC), the NOS Patch Management Team will release enterprise patch within 24 hours, with a mandated minimum 70% compliance of machines with remediation clients installed within 72 hours. If minimum compliance not met, VRO Crew will report back to 624 OC through MISREP for action to re-task or send to another unit for remediation. If compliance is 70% or greater is met, a persistent deployment will be created.

4.4 624 OPERATIONS CENTER (OC)

4.4.1 Will direct tasking Priority and Emergency remediation actions to NOS via three-tiered prioritization model as shown in Figure 4-1.

4.4.2 Will direct actions for the NOSs to cease enterprise-level patching when necessary.

4.5 690 NETWORK SUPPORT SQUADRON (NSS)/AMAC

4.5.1 Will Direct NOS, NCC/CFP and PMO through ACT to implement Normal vulnerability remediation actions via the three-tiered prioritization model as shown in Figure 4-1.

4.5.2 Will authorize NOS personnel to test software and OS updates (Ref Chapter 2).

4.5.3 Will update the associated Remedy CRQ ticket for the TCNO with relevant changes and confirm with software dashboard.

4.5.4 Compliance percentages shall be verified via vulnerability scans provided by network VATs responsible for the applicable assets (i.e., local base, PMO administrators, etc.). If delta is significant, will lead remediation actions through approved order or CRQ process.

4.6 AIR FORCE ENTERPRISE CONFIGURATION MANAGEMENT OFFICE (AFECMO)

4.6.1 Will ensure Standard Desktop Configuration (SDC) /Standard Server Configuration (SSC) versions are compliant with all applicable TCNOs/IAVMs and STIGs.

4.6.2 Will perform SDC/SSC testing and risk analysis on TCNOs/IAVMs published to the AFCYBER Readiness Center site.

4.6.3 Will report and update test and risk analysis results within 1 day of the TCNO/IAVM publish date to the AFCYBER Readiness Center site.

4.6.4 Will report and update test and risk analysis results of cumulative Microsoft patches within 2 days of the IAVM publish date to the AFCYBER Readiness Center site.

4.6.5 Will add the ARAD and SCCM Current Branch agents as permanent elements of all current and future SDC and SSC operational baselines.

4.6.6 Will create ALL SDC patch packages. The repository is the AFCEDS site: https://ceds.gunter.af.mil/

4.7 USAF NETWORK OPERATIONS SQUADRON (NOS)/CYBERSPACE OPERATIONS SQUADRON (COS) VRO

4.7.1 Will execute vulnerability remediation to reduce AFIN risk through the implementation of approved countermeasures. Countermeasures, when tasked by approved order, include, but are not limited to:

4.7.1.1 Configuration changes to systems and system registries

4.7.1.2 Installation of software patches

4.7.1.3 Removal of non-approved software

4.7.1.4 Searching for and removing malicious files

4.7.1.5 Upgrades of applications

4.7.1.6 Reinstallation of OSs

4.7.1.7 Correction of system configuration against approved configuration guidelines if the system deviates from those guidelines

4.7.2 Will create patch packages for all vulnerabilities impacting the preponderance of the AFIN to be deployed using enterprise remediation capabilities

4.7.3 Will follow the Change Management process as defined in TO 00-33A-1100, *AFNet Operational Change Management Process*, when any changes to configurations, policies, upgrades, patches, modifications or adjustments impact the performance, function or baseline configuration affecting AFNet, non-SDC and other 24 AF approved software deployments.

4.7.4 Will implement a two-phased patch testing approach before releasing AFIN-wide patches.

4.7.4.1 VROs will first issue patches to a locally developed and sourced testing environment for up to 48 hours to verify patch validity and initally determine impact to the AFIN. If issues are discovered, VROs will report these issues to the responsible party per the issued order.

4.7.4.2 If no issues are discovered, VROs will issue patches to the AFIN 3% Test Group for a period of at least 5 business days. If issues are discovered, VROs personnel will report these issues to the responsible party per the issued order.

4.7.4.3 If no issues are discovered, VROs will issue patches AFIN-wide in a persistent manner until the applicable orders are rescinded or the patch is superseded.

4.7.4.4 VROs will update the NIPR AFCYBER Readiness Center with the status of IAVM/TCNO patch development and deployment for tracking and compliance reporting purposes.
https://cs2.eis.af.mil/sites/23802/690%20NSS/crc/SitePages/IAVM_Status.aspx

4.7.4.5 Will update the associated Remedy CRQ ticket for the TCNO with relevant changes.

4.7.5 Will ensure that remediation software clients are made available for install to all endpoints connected to the AFIN. The total number of systems with operable remediation clients is the baseline for remediation compliance.

4.7.6 Will report advertisement success rate and patch compliance rate of each published TCNO/IAVM to ACT within 10 days of patch advertisement/deployment.

4.7.7 Will perform remediation using an AF-approved remote and automated remediation tool to reduce manpower and resources.

4.7.8 Will coordinate methods and procedures for PMO system patching with the PMO or system owner as requested in a Remedy CRQ.

4.7.9 Will utilize software and patch content provided by AF-approved sources as stated in applicable orders, MTOs, TOs, etc.

4.7.10 Will ensure non-Microsoft Update packages are built with uninstall or rollback programs in the event the update installation negatively affects the systems.

4.7.11 Prior to issuing test patches to the AFIN 3% Test Group, VROs will notify the responsible system owners of impending tests, test period, patch/software notes, known/expected issues, testing timeframes, affected systems and affected software and instructions on how to report issues.

4.7.12 Will collaborate with the appropriate software PMOs and notify tasking authority to seek requisite fix actions/re-tasking if remediation issues arise.

4.7.13 Will execute two types of Production Deployments:

4.7.13.1 **Mandatory Deployments** will target all machines that require the update, are not a part of an exemption and are not designated a PMO/Medical. The deployment will be made available for one day, with a deadline set at the end of the 24-hour period. The deployment will incorporate a grace period of 4 hours. Once the grace period ends, the deployment will run automatically or wait for the next available maintenance window the workstation is a part of.

4.7.13.2 **Available Deployments** will target all systems, unless stated otherwise by the tasking authority. These deployments are not mandatory. Administrators, users and PMOs will be able to log onto their respective machines and run the install.

NOTE

VRO personnel will ensure that advertisements and deployments will have mandatory assigned or deadline times for the application(s) and/or patches to run and install. All of these systems will also be targeted with a manual version of the same third-party update(s) in a manner allowing the user to run the update manually.

4.7.14 Will implement an Advertise Only Server Maintenance Window. If a server is not in a required maintenance window, it will be defaulted into the Advertise Only group. This group is primarily for mission-essential servers where a system admin must log into the server and run the installs (i.e., Core service or mission-critical servers that often need Authorized Service Interruptions (ASI) to install updates and reboot).

4.7.15 Will implement a process for users to customize an install schedule when mission requirements call for a workstation/Client system to remain uninterrupted. However, implementation deadlines shall restrict the users' ability to delay patch/software updates for an unreasonable amount of time, which is determined at the discretion of the implementation authority and VRO.

4.8 BASE-LEVEL CFP/NCC VULNERABILITY ASSESSMENT TECHNICIANS (VAT)

4.8.1 Will remediate assets owned and operated by host base personnel but not assigned to a PMO and not supported by a formal weapon systems construct by any means necessary.

4.8.2 Will ensure enterprise remediation efforts are complete before local remediation action efforts begin. Check the NIPR AFCYBER Readiness Center site for status of enterprise remediation efforts: https://cs2.eis.af.mil/sites/23802/690%20NSS/crc/SitePages/Home.aspx

4.8.3 Will perform remediation actions on any systems that are not addressed via AF enterprise remediation capabilities. Once the 95% enterprise remediation threshold is met, VAT will remediate remaining assets and/or enterprise remediation clients (e.g., SCCM, ARAD, etc.)

4.8.3.1 Bases or PMOs requiring additional patch packages (i.e., for third party or non-enterprise software or systems) will request approval for the creation of the patch package (either by the base or by the NOS) via submission of a Remedy CRQ.

CAUTION

Due to the AF implementation of SCCM Current Branch, once uploaded, patch packages are available to the entire AFIN. Therefore, it is imperative that locally-created patches are thoroughly tested and receive approval through the Change Management process.

4.8.3.2 VAT will ensure that all systems with supported OSs are able to communicate with NOS remediation tools and will work with NOS VROs for troubleshooting actions to ensure connectivity between endpoints and enterprise remediation tools.

4.8.3.3 Assets are manually updated by a technician or FSA on an individual or small group basis. In most cases these assets will require additional coordination of actions with external entities for mitigation actions and outage coordination.

4.8.3.4 DISA-compliant vulnerability scanning along with vulnerability management tool reports performed and provided by base-level VATs will validate the success of issued patches and updates.

4.8.4 Will manage vulnerabilities identified on devices that cannot be managed by NOS (i.e., non-clients) and will coordinate remediation actions with the system owners and/or administrators of those network devices.

4.8.5 Will identify PMO-controlled information systems within their respective AOR.

4.8.6 Will notify MCCC of issues arising from the testing of automated patches and create a ticket in the applicable trouble ticketing system (currently Remedy).

4.8.7 May request that systems be exempted from the regular patching schedule and moved into one of the pre-coordinated patching windows as needed and approved by 690 COG.

4.8.8 Will maintain all workstations to the current Standard Desktop Configuration (SDC) version as directed by network orders. Monthly OS updates cannot be guaranteed to work with any SDC version that is based on a build of Windows that Microsoft does not support.

4.9 PROGRAM MANAGEMENT OFFICE (PMO)

4.9.1 Will remediate assets that are supported by a weapons system or program management office.

NOTE

Mitigation efforts are only authorized via Change Requests (CRQ) from the PMO. Changes to these assets cannot occur unless authorized and directed by PMO.

4.9.2 Will coordinate vulnerability remediation on servers, within their respective AOR with NOS until acceptable compliance levels are achieved. These compliance levels are based of the total number of systems with active and operable remediation clients. Goals for remediation are set by the PMO.

NOTE

Vulnerabilities identified on devices that cannot be managed by NOS (i.e., non-clients) are the responsibility of the system owners and/or administrators of those network devices.

4.9.3 May utilize patch-exempt groups to isolate systems from AFIN-wide patches and updates.

4.9.4 Shall ensure that all systems with supported OSs are able to communicate with NOS remediation tools and will work with NOS VROs for troubleshooting actions to ensure connectivity between endpoints and remediation tools.