

PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

PURPOSE:

Develop a process for managing software upgrades/patches on FDA regulated medical devices; specifically focusing on Department of Defense (DoD)-Vendor process for checking validity, testing, and recommending how security issues covered in Computer Emergency Response Team (CERT), Time Compliance Network Orders(TCNO), security notices, etc. (herein inclusively called “patch/update management”) should be applied to vendor-specific medical devices.

BACKGROUND:

- Broad-based Health Information Systems (HIS) and “specialty” systems such as Radiological Information Systems (RIS) have greatly increased over the last ten years
 - Moving from islands of technology to internet-enabled networks, the quality of patient care has increased, but at the price of data/information being vulnerable to attacks by hackers/viruses
- Every computer connected to a network is vulnerable to attacks by hackers trying to gain access for a range of purposes from “just looking around”, to inserting malicious logic (virus) for the purpose of altering, destroying or adding data to individual computers or entire networks
 - Though not unique to DoD, “industrial secrets”, Privacy Act, and national security information on DoD computers/networks compound the need to properly manage network security
 - The issue further complicated on Health Information Systems (HIS) containing patient data
 - Health Information Portability Accountability Act (HIPAA) guidelines
 - Protected Healthcare Information (PHI) management requirements becoming more stringent
- Hacker and malicious logic defenses include physical security, user training, network security software, anti-virus software, operation system (OS) & application software patches, etc.
- DoD/Services have detailed “defensive” procedures to mitigate the effects of hackers/viruses; but a great challenge remains in managing vulnerabilities caused by insecure software designs
- There are two main sources for notices/solutions for software/network security breaches:
 - Software vendors identify security problems in software, create patches and notify users
 - Carnegie Mellon Software Engineering Institute’s Computer Emergency Response (CERT) Team, which reviews vendor notices on security vulnerabilities, identifies new software vulnerabilities, provides solutions for vulnerabilities, and provides solutions for actual network security breaches
- The primary management process for security patches in DoD flow from information/solution from the CERT Command Center down through the DoDCERT chain-of- command
 - [CERT/CC: CERT Coordination Center](#)
 - [US-CERT: New Department of Homeland Security, and National Cyber Security Division Initiative](#)
 - [DoD-CERT: Department of Defense Computer Emergency Response Team](#)
 - [ACERT: Army Computer Emergency Response Team](#)
 - [AFCERT: Air Force Computer Emergency Response Team](#)
 - [NAVCIRT: Navy Computer Incident Response Team](#)

MEDICAL DEVICE ISSUES:

- Today there is a “blurring” between HIS and FDA regulated medical devices on the network
 - i.e. Picture Archiving and Communications Systems (PACS), tele-radiology systems, tele-dermatology systems, etc., though hooked to the network, are FDA regulated medical devices
- Networked FDA regulated medical devices have the same vulnerabilities to hackers and viruses, however, these medical devices require a different approach to management of security patches
 - Installation of “vendor unapproved” security patches can not only crash the system, but relive vendors of any liability due to patient misdiagnosis, damage to modalities, or patient death

PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

RECOMMENDATIONS:

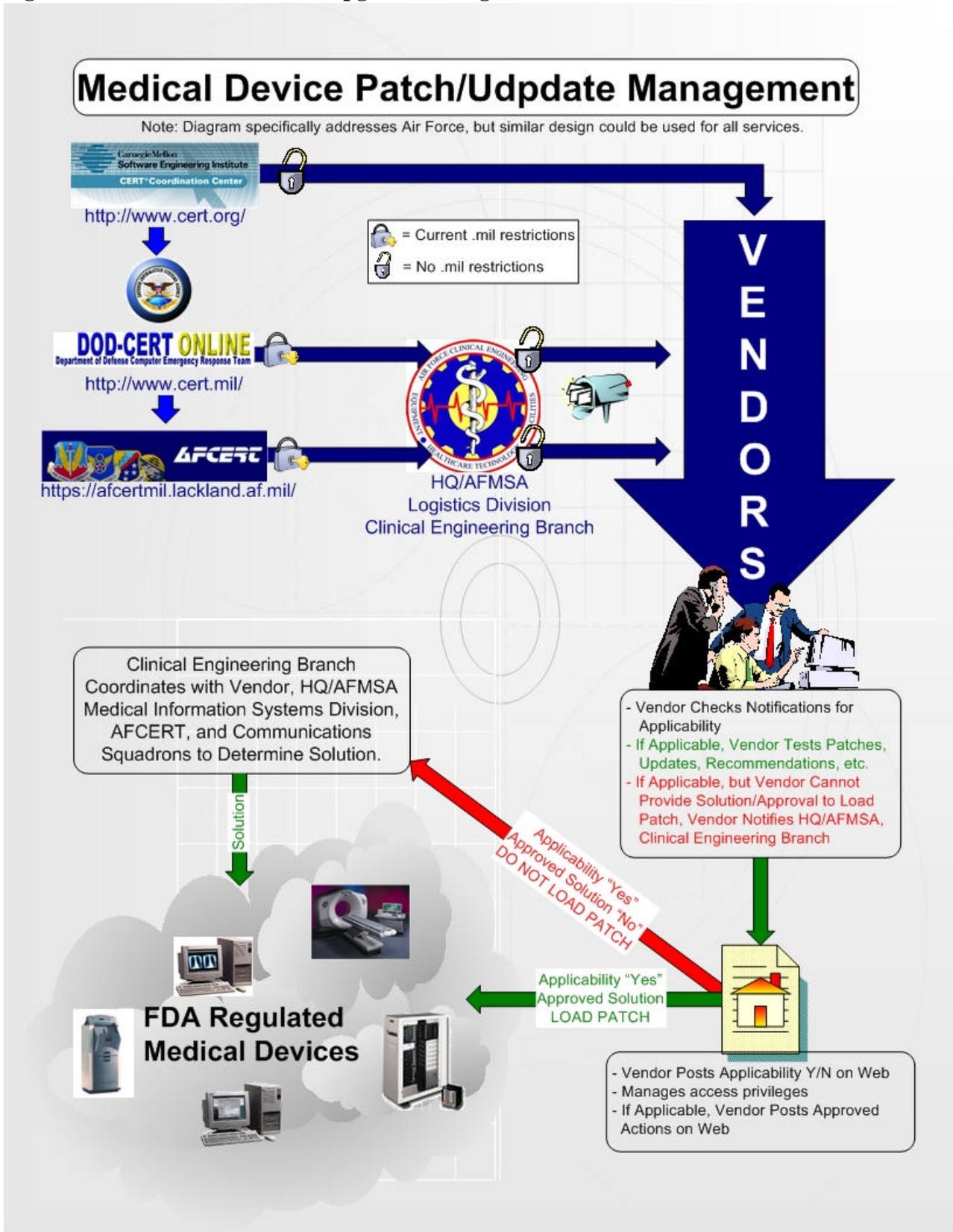
- No change to the current process for PCs connecting to medical devices/archives via web browsers
- New processes must be put in place to validate, test, and provide vendor recommendations for applying security patches prior to installation on FDA regulated medical devices/systems
 - Vendors of FDA regulated medical devices and Military Health System (MHS) staff must be proactive in designing an appropriate process to manage the security patches
 - Vendors must recognize this is not a “DoD” issue; civilian organizations hold the same liability
- Network segmentation of FDA regulated medical devices would bridge the “gap” between time-sensitive critical update deadlines and the time required for medical device vendors to test/approve updates
- Recommended Process: (Figure 1)
 - “Vendor Security Team” subscribes to [CERT Advisory Mailing List](#)
 - DoD Service POCs (i.e. HQ/AFMSA-Clinical Engineering Branch in AF) should forward DoD/Service specific CERTS/Notices to Vendor Security Team; this is an interim measure until the Vendor Security Teams can gain approval for receiving DoD/Service CERTs
 - Upon receipt of advisory, vendor should check applicability of CERT (cross reference CERT) to vendor’s medical devices; applicability should be immediately noted on vendor web site (Figure 2)
 - If CERT does not impact any of the vendor’s medical devices, then a simple notation on the web site would finalize actions on the security update
 - If CERT is applicable to any supported medical devices, then security update testing should begin in a priority-based method with approved solutions being posted on the vendor’s web site
 - If testing indicates security patch cannot be installed on a device, vendor will notify DoD Service POCs who will work with appropriate agencies to formulate an acceptable solution
 - Prior to installing security patches on any medical device, information systems/medical staff will check the vendor web site for approved solution to CERT notifications
- **BOTTOM LINE**—No security patches should be loaded on FDA regulated medical devices prior to vendor approval

SOURCES FOR DEVELOPING CERT PROGRAMS:

- Subscribe to CERT Advisory Mailing List: http://www.cert.org/contact_cert/certmaillist.html
- Presentations about CERT and Processes: <http://www.cert.org/nav/present.html>
- Computer Security Incident Response Team (CSIRT) Development <http://www.cert.org/csirts/>

PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

Figure 1: Medical Device Patch/Upgrade Management Flowchart



PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

Figure 2: Medical Device Patch/Upgrade Management Flowchart : Recommended Inclusions for Vendor Web Sites

Medical Device Patch/Update Management

Recommended Inclusions for Vendor We-Based Tracking



Vendor Name



Vendor Logo/Info

Note: Latest Item at Top of Table

 Vendor Contact E-mail

Medical Device Patch/Security Update Applicability Chart

						
CERT/CC	DoD CERT	ACERT	AFCERT	NAVCIRT	Applicable	Solution Status
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✗	[REDACTED]

"Privacy Notice" or other vendor release information.

Ref# Number for CERT, AFCERT, TCNO, etc. (Red signifies a Critical Level Item)

Ref# Reference Should link, where access is not blocked, to the actual notices.

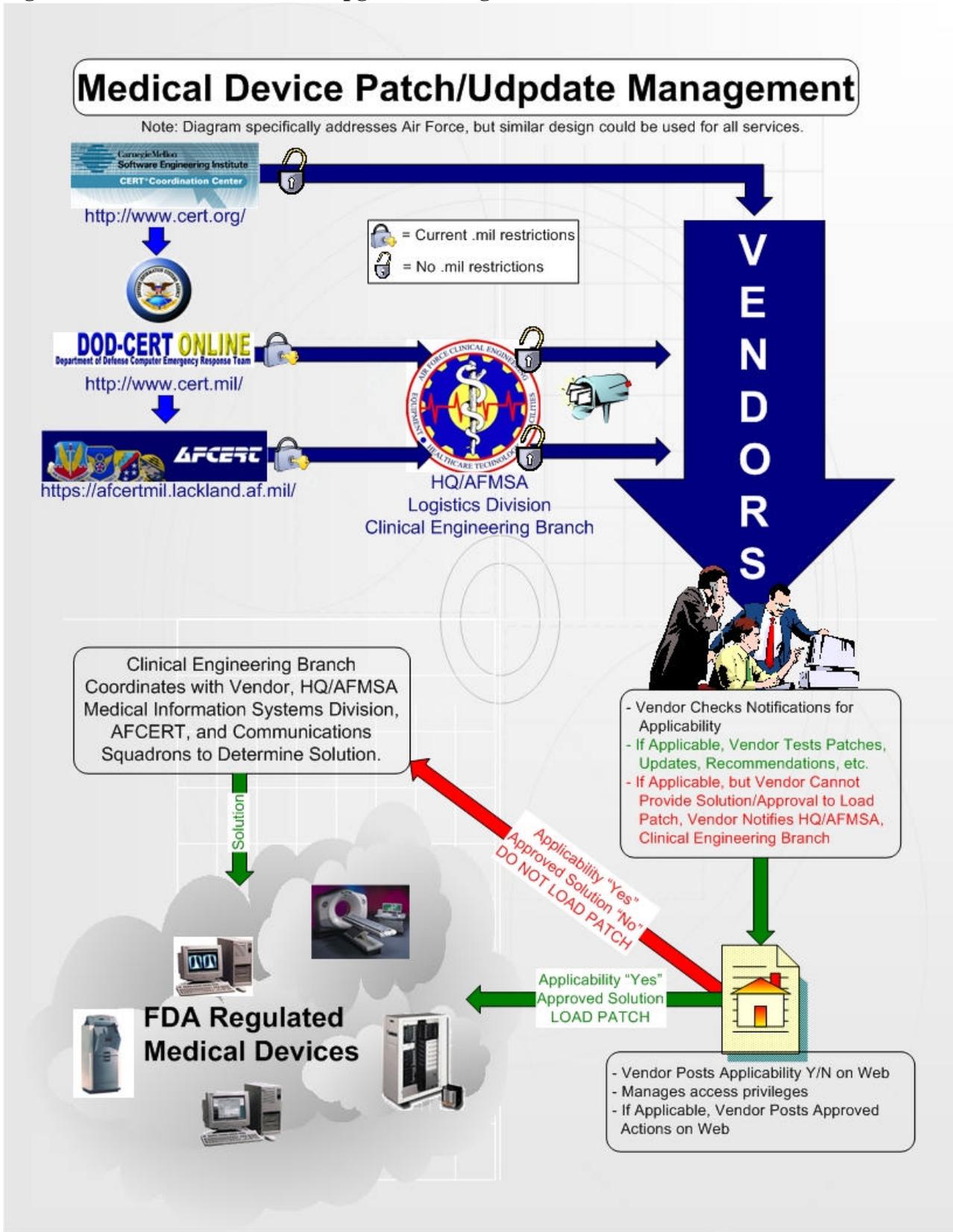
 Applicable to At Least One Product...Link from this cell should list all products that affected.

 Not Applicable to ANY of Vendor's Products

-  None of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility.
-  Part of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility. Link should take user to page where update/patch guidelines are explained. (To avoid duplication of work, vendor may simply list devices and indicate CERT/AFCERT/etc. guidelines may be followed.)
-  All of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility. (See note above for link information.)

PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

Figure 1: Medical Device Patch/Upgrade Management Flowchart



PATCH MANAGEMENT FOR FDA REGULATED MEDICAL DEVICES

Figure 2: Medical Device Patch/Upgrade Management Flowchart : Recommended Inclusions for Vendor Web Sites

Medical Device Patch/Update Management

Recommended Inclusions for Vendor We-Based Tracking



Vendor Name



Vendor Logo/Info

Note: Latest Item at Top of Table

 Vendor Contact E-mail

Medical Device Patch/Security Update Applicability Chart

						
CERT/CC	DoD CERT	ACERT	AFCERT	NAVCIRT	Applicable	Solution Status
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✓	
Ref#	Ref#	Ref#	Ref#	Ref#	✗	[REDACTED]

"Privacy Notice" or other vendor release information.

Ref# Number for CERT, AFCERT, TCNO, etc. (Red signifies a Critical Level Item)
Ref# Reference Should link, where access is not blocked, to the actual notices.

 Applicable to At Least One Product...Link from this cell should list all products that affected.
 Not Applicable to ANY of Vendor's Products

-  None of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility.
-  Part of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility. Link should take user to page where update/patch guidelines are explained. (To avoid duplication of work, vendor may simply list devices and indicate CERT/AFCERT/etc. guidelines may be followed.)
-  All of the Applicable Applications/Systems have been Tested for Patch/Upgrade Compatibility. (See note above for link information.)