VETERANS AFFAIRS HEALTHCARE TECHNOLOGY MANAGEMENT

Medical Device Protection Program

Meaghen Krebsbach Supervisory Biomedical Engineer, Milwaukee VAMC
Connor Walsh Director, Networking & Cybersecurity, Office of HTM

MDEXPO
New England • October 8-10, 2024

Agenda | Medical Device Protection Program

1 VA AND MEDICAL DEVICE SECURITY OVERVIEW

2 VA MEDICAL DEVICE PROTECTION PROGRAM

3 TAKEAWAYS AND DISCUSSION

Overview | Mission and Vision

U.S. Department of Veterans Affairs

HTM

Healthcare Technology Management

MISSION

Honor Veterans by developing and guiding comprehensive management of healthcare technologies to assure safe, available, and innovative medical technology used to deliver exceptional health care for Veterans.

VISION

Be an efficient, innovative and customer-oriented Center of Excellence that continually enhances VHA's ability to deliver world class health care for our nation's Veterans through exceptional management of healthcare technology as well as position VHA as the national leader healthcare technology management in the healthcare industry.

US Department of Veterans Affairs (VA) Healthcare Technology Management (HTM)

Overview | VA HTM by the Numbers

1 CENTRAL OFFICE

18 VETERAN INTEGRATED SERVICE NETWORKS

171 MEDICAL CENTERS

$10 billion
of healthcare technology

900,000
medical devices and clinical systems

155,000
network connected medical devices

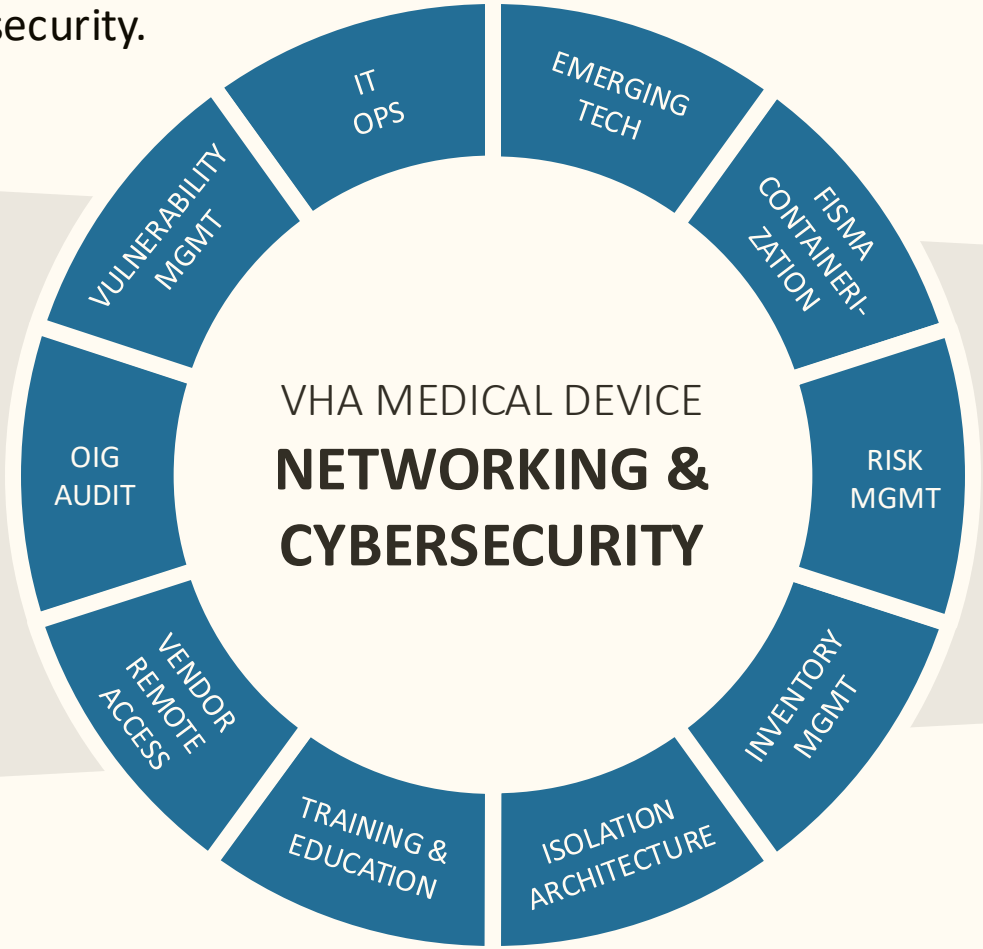
2,200
Biomedical Engineering professionals

MDEXPO
New England • October 8-10, 2024

Overview | Medical Device Protection Program

VA's MDPP is a comprehensive security initiative intended to better safeguard network-connected medical devices and mitigate risks to patient safety and cybersecurity.

MDPP
Medical Device Protection Program

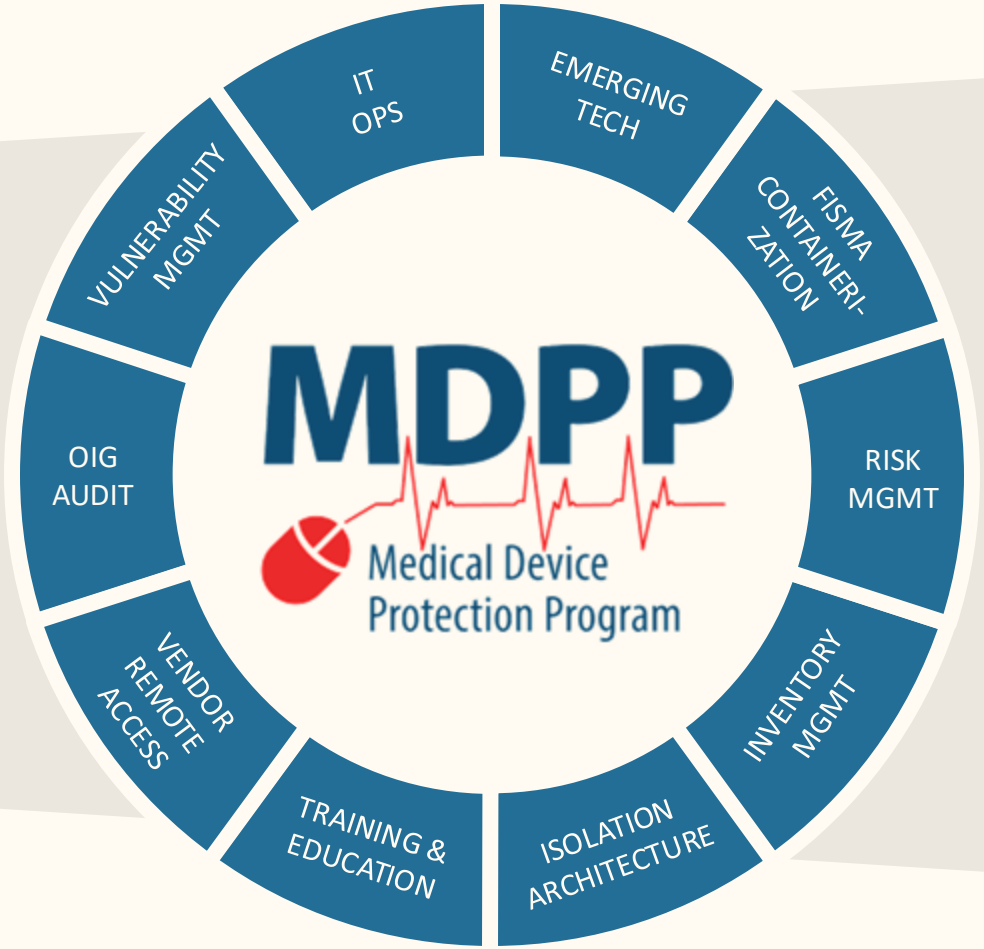


Overview | Medical Device Protection Program

2024 MEDCRYPT CYBERSECURITY VISIONARY AWARD WINNER! | AAMI

VHA HTM relies on the **field-based subject matter experts** who volunteer as members of the MDPP

- **3** Office of HTM FTEE
- **10** subgroups
- **90+** members
- **60+** unique members



Centralized **patch approval repository** with 7,000 entries

Standardized inventory of networked devices and clinical systems

Full suite of **medical device standards and policies**

Robust **tracking and reporting** of **vulnerabilities**

Annual cybersecurity **audit readiness program**

Medical Device Protection Program | Risk Management

ENTERPRISE RISK ANALYSIS

Requires VA HTM and manufacturer input for all VA networked medical devices and systems

- **Identifies the inherited risk and impact to the VA**
- **Documents and addresses system specific security controls**
- **Manages and addresses vulnerabilities**

1 VA 6550 APPENDIX A

VA-specific pre-procurement assessment form for cybersecurity features, such as FIPS 140-2 or 140-3 certification, antivirus and OS patching, data encryption capabilities and electronic health record compatibility.

2 MANUFACTURER DISCLOSURE

Standard document -- Manufacturer Disclosure Statement for Medical Device Security (MDS2) -- for manufacturers to communicate cybersecurity information about their equipment.

3 INVENTORY LIST

Listing of device name, type, model, operating system, operating system version, and software application name and versions for all networked devices and peripherals within the system.

4 PORTS & PROTOCOLS

Listing of Ports, Protocols, and Services (PPS) to record communication service (SMTP, DNS, DICOM, Custom Comms, etc.), port numbers, protocol (TCP, UDP, IP), communication direction, external IP communications, and reason for use.

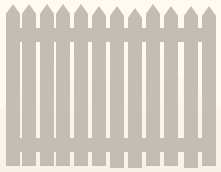
5 NETWORK TOPOLOGY

Diagram showing Accreditation Boundary of the system, all directional communication services as identified by the PPS, and any communications to systems outside of the VA network.

Medical Device Protection Program | Isolation Architecture

MEDICAL DEVICE ISOLATION ARCHITECTURE

VA segregates its network-connected medical devices from the internal, VA enterprise network by utilizing **Virtual Local Area Networks** (VLANs) and protecting them with **Access Control Lists** (ACLs) or **Firewalls**.



VLANs

Network segmentation

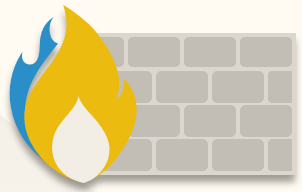
Logically divides a single physical network into multiple virtual networks

Each VLAN operates as a separate broadcast domain, allowing for segmentation and isolation of network traffic

ACLs

Basic traffic filtering

Control traffic flow on routers and switches based on predefined rules that filter certain source/ destination IP addresses, protocols, ports, etc.



FIREWALLS

Beyond basic traffic filtering

Offer advanced security features, threat detection, and adaptive capabilities to safeguard networks against evolving cyber threats

Medical Device Protection Program | Inventory Management

An **accurate**, **complete**, and **uniform** inventory is foundational to a successful HTM program

155,000
network-connected medical devices within VA!

ASSET INVENTORY

VA's homegrown **Networked Medical Device Database (NMDD)** is the authoritative source for VA's network-connected medical device inventory.

NMDD documents device operating systems, ERA identification numbers, MAC addresses, software inventories, etc.

NAMING STANDARDS

VA's **Medical Device Nomenclature Standards (VA-MDNS)** and **Naming Standards Index (NSI)** establish standards for naming devices and systems.

VA-MDNS establishes consistent category and model naming for devices while NSI applies to clinical systems and links to ERAs.

KPIs measuring compliance

- Percent of **VLANs** within the **inventory**
- Percent of **devices** within the **inventory**
- Percent of **devices** with **std. category**
- Percent of **devices** with **std. model**
- Percent of **devices** with **sufficient data**

Medical Device Protection Program | IT Operations

HTM IT OPERATIONS
CHECKLISTS

VA uses a series of checklists to guide the VA HTM community through medical device security responsibilities across the medical device lifecycle.

Provides easy-to-follow, sequential steps in online or printable formats.

Documents application of cybersecurity processes and controls, related ticket and work order numbers, and field notes.

Links to relevant policies, tools, and resources for easy reference.

VA HTM reviews and updates its medical device cybersecurity service bulletins at least bi-annually.

IMPLEMENTATION

- Complete post-award security implementation
- Receive and inventory equipment
- Configure network and organizational unit
- Configure vendor remote connection (if required)
- Configure operating system
- Install application software
- Document medical device in NMDD

SUSTAINMENT

- Obtain elevated privileges for admin. access on domain-joined systems
- Ensure encryption of service laptops or implement mitigating controls
- Scan mobile media prior to attaching to the medical device
- Perform Planned Maintenance procedures as scheduled
- Monitor ACLs and comply with change mgmt. processes
- Report and respond to cybersecurity incidents
- Establish disaster recovery and contingency plans

DECOMMISSIONING

- Sanitize device's electronic storage media
- Turn in device to Logistics
- Update/delete medical device records in NMDD
- Request IT actions and cleanup

Medical Device Protection Program | FISMA Containerization

RISK MGMT
ISO ARCHITECTURE
INVENTORY MGMT
IT OPERATIONS
CONTAINERIZATION
OIG AUDIT
VUL MGMT
REMOTE ACCESS
TRAINING & EDU
EMERGING TECH

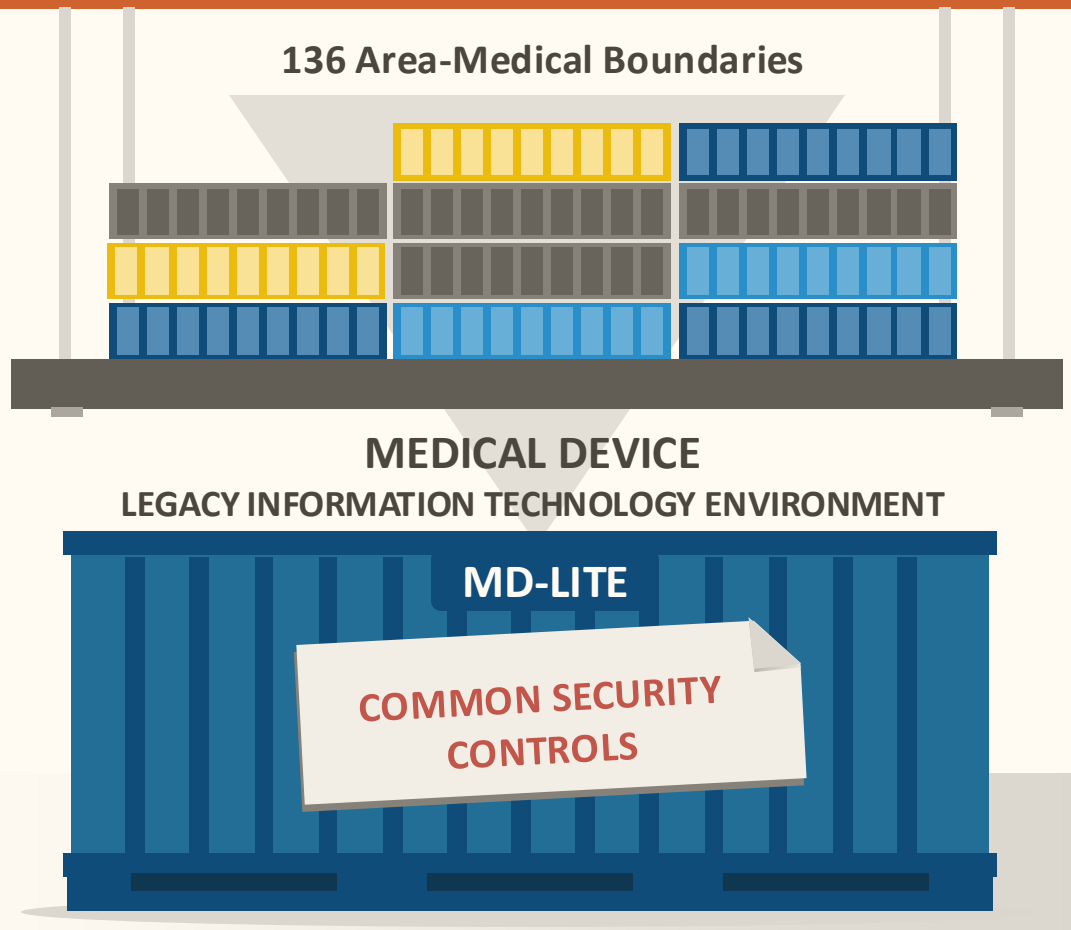
FISMA

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Requires each federal agency to develop, document, and implement an information security program

All networked devices must be included in the **Enterprise Mission Assurance Support Service (eMASS)** for inventory tracking and reporting.

Assets are assigned to different boundaries within eMASS and require documentation to demonstrate compliance with the security controls and achieve authorization to connect.



Streamlines Security Processes

Improves Governance

Allows For Enterprise-level Plans of Actions & Milestones
POA&Ms

Medical Device Protection Program | OIG Audit

The VA Office of Inspector General (OIG) randomly selects VA medical centers for its annual FISMA/Federal Information System Controls Audit Manual (FISCAM) audit of all devices connected to the VA network, specifically related to configuration, security, back-up, disaster recovery, etc.

VA HTM **prepares every VA medical center** for audit through annual completion of deliverables

AUDIT PREP DELIVERABLES AND NIST CONTROLS

1. Memo to appoint media sanitization personnel	MP-6
2. Example of completed Enterprise Risk Analysis (ERA)	RA-3
3. Medical equipment management plan	MA-6
4. CM and PM schedule and equipment history	MA-4
5. Audit log for two medical devices	AU-2
6. Access authorization to HTM and IT computer rooms	PE-2
7. Vendor visitor check-in log	PE-8
8. HTM and IT server room visitor logs	PE-8
9. One-month scanning station scan log	MA-3
10. Photo of HTM scanning station	MA-3
11. Remediation log of all medical device vulnerabilities	SI-2
12. Networked inventory compliance and conformance report	CM-8
13. Updated medical device inventory	N/A
14. ACL remediation log/tickets	SC-7
15. Remote Access Portal (RAP) log	CA-3

Medical Device Protection Program | Vulnerability Management

RISK MGMT
ISO ARCHITECTURE
INVENTORY MGMT
IT OPERATIONS
CONTAINERIZATION
OIG AUDIT
VUL MGMT
REMOTE ACCESS
TRAINING & EDU
EMERGING TECH

VULNERABILITY MANAGEMENT

VA takes a multi-faceted approach to tracking, reporting, and addressing vulnerabilities

RISK ASSESSMENT
Evaluation and acceptance of risks of each networked medical device BEFORE it's connected to the network

SERVICE MANAGEMENT SYSTEMS
Modernization of HTM service management systems for tracking vulnerability management functions

ISOLATION ARCHITECHTURE
Separation of networked medical devices from the internal, VA enterprise network

TECHNICAL CONFIGURATION
Standardization of optimized clinical system configurations to limit vulnerabilities

SMAK INFORMATION
Automated collection of critical system information with linkage to networked medical device inventory

PATCH REPOSITORY
Centralization of clinical system patch approvals, inclusive of 26 manufacturers and 7,000 entries

UNSUPPORTED OPERATING SYSTEMS
Identification and replacement or mitigation of devices running on unsupported operating systems

VULNERABILITY REMEDIATION
Identification, acknowledgement, and remediation of known medical device cybersecurity vulnerabilities

Medical Device Protection Program | Vendor Remote Access

VA HTM ensures vendors use an approved and appropriate remote connection to support medical devices. Impacts to existing infrastructure and operations, hardware and software requirements, data sensitivity, and security controls are considered when implementing new connections.

Site-to-Site

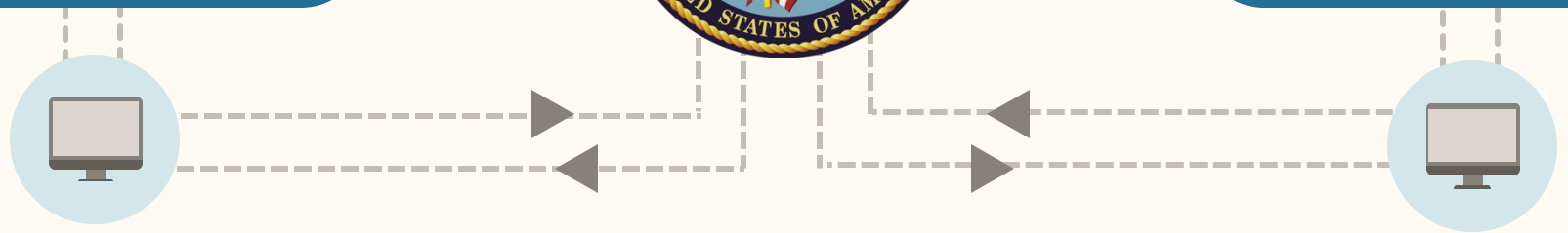
S2S

a connection with multiple users from the same business partner with an MOU/ISA

Client-to-Site

C2S

a connection with a single remote user when there is no S2S connection



Medical Device Protection Program | Training & Education

VA offers HTM cybersecurity staff a robust **professional development program** to safeguard technology, build their capabilities, and advance in their careers.

COURSES

Live in-person and online full-day+ training courses

WEBINARS

Recorded webinars and short-form **HTM Bytes** videos

CERTIFICATIONS

Prep **courses**, **coaching**, and **vouchers** for HTM certifications

COURSE CATALOG

CYBERSECURITY & NETWORKING

HTM111: **Introduction to Cybersecurity**

HTM112: **Basic Networking for Biomedical Staff**

HTM115: **Windows Server**

HTM211: **Introduction to Operating Systems & SQL**

HTM212: **Intermediate Networking**

HTM213: **Introduction to Virtual Machines**

HTM214: **Principles of HTM Cybersecurity**

PANED210: **Firewall Essentials**

HTM311: **DICOM Fundamentals**

HTM312: **Introduction to HL7**

Medical Device Protection Program | Emerging Technologies

VA HTM continuously identifies, researches, evaluates, implements, and utilizes emerging technologies to better secure medical devices/systems.

NETWORKED DEVICE VISIBILITY TOOL

- Asset Management
- Asset Discovery
- Vulnerability Management
- Network Analysis
- Data Visualization

SIM LEARN LAB

- Hyperconverged Virtual Stack
- Virtual Server Catalog
- Penetration Testing

Medical Device Protection Program | Programmatic Priorities

MDPP Medical Device Protection Program

OVERARCHING PRIORITIES

1. Strengthen **communications** with VA HTM field
2. Build **relationships** within VA and with industry and fellow agencies
3. Recruit and retain skilled **HTM cybersecurity professionals**

Discussion

Connor Walsh
Director, Network & Cybersecurity
Office of Healthcare Technology Management

Meaghen Krebsbach
Supervisory Biomedical Engineer
Milwaukee VAMC

NMDD Screenshot | VLAN

VLAN

Search VLANs: Search term...

Number ASC / DESC	Common Name ASC / DESC	Location ASC / DESC	Beginning Host ASC / DESC	Ending Host ASC / DESC	Subnet Mask ASC / DESC
273	AbbottLink	Building 2 Lab			255.255.255.240
242	Audioscan Verifit	Audiology			255.255.255.224
274	Beckman ACLTOP 500	Building 2 Room 152			255.255.255.240
22	BED-CARESTREAM-PACS-22	VA Bedford			255.255.255.224
275	Bedford Cepheid Lab	VA Bedford Lab			255.255.255.240
65	Bedford GE Holter	VA Bedford			255.255.255.240
268	Bedford NATUS / XLTEK	VA Bedford			255.255.255.240
25	Bedford Omnicell	VA Bedford			255.255.255.128
141	Bedford Philips-Xcelera	VA Bedford			255.255.255.224

NMDD Screenshot | Devices

Devices

Information

VLAN Number	25
VLAN Name	Bedford Omnicell
ACL Name	MDIA-BED-OMNICELL_PHARM-25
VLAN Range	
DHCP	False

Show ACL | Show VLAN Info

Actions

Turn On DHCP | Select All Devices for Deletion | Delete All Selected | Export IP Grid | Show VLAN Lookup | Reload Grid

Total IPs in VLAN: 128
Available IPs in VLAN: 99

Search Grid: Search term...

Delete		IP Address ASC / DESC	SMAK	RAP Portal	Naming Standard Index (NSI)	ERA Number (Legacy Field)	Network Name ASC / DESC	Location ASC / DESC	MAC Address ASC / DESC	EE/MX ASC / DESC	Description ASC / DESC	OS ASC / DESC	Responsible Staff ASC / DESC	*beta* Last Seen On Network *beta*	Modified By ASC / DESC	Modified Date ASC / DESC	ID
	Details		False		10053	Pre-ERA		B15-78				Windows Embedded Standard (Windows 7)		9/19/2024 (scans can be delayed)		4/27/2024 12:22:31 AM	918607
	Details		False		7339	Pre-ERA		B15-78				Proprietary Embedded		9/19/2024 (scans can be delayed)		4/10/2024 8:21:02 AM	918612
	Details		False		10053							Windows 10		*not scanned yet* (scans can be delayed)		4/1/2024 2:30:55 PM	1512352

NMDD Screenshot | Device Detail

Device Detail

IPAddress	
ReservedAddressTypeText	
ERANumber	PRE-ERA
SMAK	☑
Network Name	
Location	
MacAddress	
EE	
SerialNumber	
Description	Omnicell Server WorkflowRx
ResponsibleTech	
EquipmentCategory	SERVER-ADP
Manufacturer	OmniCell
PhysicalManufacturer	DELL COMPUTER

Model	E18S
DeviceOU	
OperatingSystem	Windows Server 2012r2
OSPatchingRegimen	All Patches applied from HTM MDUS server
DeviceFunction	MDUS Patching w/ exclusions
Wireless	☐
Virtual	☐
Laptop	☐
Encrypted	☐
Is on VA Domain	☐
Production Status	
PHI	
DHCP	☐
BackedUp	☐

AVManufacturer	McAfee 8.8
AVPatchingRegimen	MDUS Patching w/ exclusions
VPNAccess	Yes - Site-to-Site
DataPort	
Switch	
SwitchClosetRoom	
WallJackNumber	
NatIP	
AETitle	
CreateByDisplay	
CreateDate	4/10/2015 11:31:18 AM
ModifiedByDisplay	smak link
ModifiedDate	12/28/2023 4:17:00 PM

Software:

Software Name	Software Version	Comments

VA Directive 6550 | Appendix A

VA DIRECTIVE 6550 Appendix A

To be completed for all procurements of network-connected medical devices and non-network-connected medical devices that store sensitive information. For client/server systems, a separate 6550 Appendix A is required for each the client and the medical server.

1.1	Equipment Category (VA-MDNS)	
1.2	Manufacturer	
1.3	Model	
1.4	NSI Number (if known)	
1.5	Application Name and Software Version #	
1.6	Requesting Service	
1.7	VISN	
1.8	Facility Name	
1.9	Facility Number	
1.10	Manufacturer Point of Contact	
	Phone Number	
	E-mail address	
1.11	Biomedical Engineering Point of Contact	
	Phone Number	
	E-mail address	
1.12	Responsible Service if Biomedical Engineering is NOT the Primary System Manager for system maintenance, support and lifecycle management	
1.13	Medical Device Type	☐ Discrete device ☐ Software ☐ Client ☐ Application server

1.14	Device Description (i.e. equipment function and systems it communicates with)	
1.15	MDIA VLAN Number for installation (if known)	
1.16	Device Operating System (OS) *Please include OS build level.* *Review support status for **Windows OS** versions here.*	
Procurement of devices with unsupported operating systems is prohibited. Unsupported operating systems are OSs that are not supported by the manufacturer and have reached the end of the OS lifecycle as published by the OS manufacturer (i.e. no further security patches will be released for the OS by the manufacturer after the OS end-of-life nor will be available by other methods such as extended warranty purchases from the OS manufacturer).		
1.17	Does the device support wireless network connection?	☐ Yes ☐ No
	If yes, what is the FIPS 140-2 or 140-3 certification number?	
	If no, does the vendor support the installation of FIPS 140-2 or 140-3 wireless cards?	☐ Yes ☐ No
Procurement of devices using 802.11 wireless networking that are not FIPS 140-2 or 140-3 compliant is prohibited.		
1.18	Does the device have an existing, active Enterprise Risk Analysis (ERA)?	☐ Yes ☐ No
	If yes, what is the ERA number?	
	If the device has a direct connection to Cerner or **EHRM interface**, does the device have an existing **MedMod ERA**?	☐ Yes ☐ No
	If yes, what is the **MedMod ERA** number?	
	***Note that the ERA must be for the same make, model, and application software version to apply to the requested device. A new ERA is required for major software or operating system updates (e.g. version 2.0 to 3.0) but is not required for minor updates (e.g. version 2.0 to version 2.1).*	
If an ERA exists for the requested device, completion of the 6550 Appendix A is not required beyond this point. Please sign to certify that an existing ERA is available for the requested device and forward the document to either the Area Manager or ISSO for signature, as appropriate. Please note that if the device is an EHRM device, a MedMod ERA is required.		

VA Directive 6550 | Appendix A

2.1	Can the OS be automatically patched?	☐ Yes ☐ No
	***Note that devices that do not support automated patching via the VHA MD Update Server (MDUS) or via vendor channels impose a significantly higher risk to the VA network.*	
	If patching is not automated, what is the patching process and/or limitations?	
2.2	For applications and sub-applications (e.g., Java, Apache) on the device, is automatic patching or updating supported?	☐ Yes ☐ No
	***Note that devices that do not support automated patching impose a significantly higher risk to the VA network.*	
	If patching is not automated, what is the patching process and/or limitations?	
2.3	Is a device hardening guide available?	☐ Yes ☐ No
2.4	Does the device have logging or other auditing mechanisms in place?	☐ Yes ☐ No
	If yes, can these logs be exported to a syslog or similar server?	
2.5	Does the device include a database?	☐ Yes ☐ No
	If yes, what is the database version and type (e.g., SQL, Oracle)?	
	***Note that procuring and deploying devices with unsupported database versions imposes a significantly higher risk to the VA network.*	
	Does the vendor support database conversion from SSN to electronic data interchange personal identifier (EDIPI)?	☐ Yes ☐ No ☐ No PHI
	Does the vendor database support multiple identifiers?	☐ Yes ☐ No ☐ No PHI
2.6	Can the device run Defender, ESET, or McAfee antivirus?	☐ Yes ☐ No
	***Note that devices that do not support VA-approved antivirus scanning or an antivirus scanning solution managed by the vendor impose a significantly higher risk to the VA network.*	
	If antivirus is not supported, what are the AV processes and/or the limitations?	

2.7	Can a commercial-off-the-shelf (COTS) endpoint management system be installed (e.g., IBM Big Fix, Goverlan, SCCM)?	☐ Yes ☐ No
	If so, which one(s)?	
2.8	For Windows-based devices, can the existing Microsoft service be enabled to communicate with the VHA SMAK-AM server?	☐ Yes ☐ No ☐ Non-Windows-based system
	If no, has the vendor agreed to provide a complete software and application inventory for all system components as per FISMA requirements?	☐ Yes ☐ No
	***Note that devices that do not support communication with the SMAK-AM server or for which the vendor does not agree to provide a complete software inventory impose a significantly higher risk to the VA network.*	
2.9	Does the device support the use of two-factor authentication?	☐ Yes ☐ No
	***Note that devices that do not support two-factor authentication impose a significantly higher risk to the VA network. Please review the VA's requirements for two-factor authentication here.*	
	Does the device require interactive login service accounts?	
	***Note that devices that require interactive login service accounts impose a significantly higher risk to the VA network.*	
2.10	Will the device be joined to the VA domain?	☐ Yes ☐ No
	***Note that devices that are not joined to the domain impose a significantly higher risk to the VA network.*	
2.11	Does the device allow for encryption of the data drive or OS drives?	☐ Yes ☐ No
	What level of encryption is allowed?	
2.12	Are post-quantum cryptography (PQC) ciphers being used for this implementation?	☐ Yes ☐ No

VA Directive 6550 | Appendix A

2.13	What method of encryption is used for data in transit?	☐ SSL ☐ HTTPS ☐ TLS (version: _____) ☐ SFTP ☐ None ☐ Other:
	***Note that use of SSL is prohibited and that TLS versions 1.0/1.1 impose a significantly higher risk to the VA network.*	
2.14	Is sensitive data stored at rest on the device?	☐ Yes ☐ No
	If yes, how many records can be stored on the device?	☐ <500 ☐ >500
	If yes, does the device support on demand purging of data from the local hard drive?	☐ Yes ☐ No
2.15	Will sensitive data be stored outside of the VA network (e.g. cloud-based service provider – excludes Electronic Medical Record connection)?	☐ Yes ☐ No
2.16	Does the device send/receive VA data to/from an external, vendor-managed cloud?	☐ Yes ☐ No
	If yes, has the cloud platform been approved by the VA Digital Transformation Center (DTC)? *To determine approval status, please visit the Digital VA Product Marketplace.*	☐ Yes ☐ No
	If yes, what is the cloud type, determined by the VA DTC?	☐ Software as a Service (SaaS) ☐ Managed Service
	If SaaS, what is the FedRAMP package ID?	
	If SaaS, is it FedRAMP authorized?	☐ Yes ☐ No
	Is there an approved VA ATO for the cloud platform?	☐ Yes ☐ No

2.17	Is connectivity external to the VA required for device operation?	☐ Yes ☐ No
2.18	Is connectivity external to the VA required for device support?	☐ No ☐ Yes - VA S2S VPN ☐ Yes - VA Citrix ☐ Yes – VA Azure Virtual Desktop ☐ Yes – Other
	If other, describe the remote access method.	
	What is the MOU/ISA number?	
2.19	How many IP addresses are required?	
2.20	What kind of IPs does the device use?	☐ Static IP ☐ DHCP
	***Devices should be deployed with static IPs unless DHCP is required.*	
2.21	Is IPv6 supported?	☐ Yes ☐ No
	If yes, please list any limitations.	
2.22	If server-based, select one from each column:	☐ Vendor-provided ☐ VHA-provided ☐ Other - describe ☐ Physical server ☐ Virtual host ☐ Cloud virtual host
2.23	If server-based, list server specifications (cores, RAM, power, storage) and rack space. *Attach additional documentation, as needed.*	
2.24	Does the device use Java?	☐ Yes ☐ No
2.25	Does the device utilize machine learning/artificial intelligence?	☐ Yes ☐ No
2.26	What type of vulnerability scanning is allowed on the device?	☐ Active ☐ Passive ☐ Both
	If active, is credentialed scanning allowed?	☐ Yes ☐ No

VA Directive 6550 | Appendix A

2.27	If the device uses digital signatures, is it compliant with FIPS 186-4?	☐ Yes ☐ No ☐ N/A
2.28	Does this system include a pre-production (test) environment?	☐ Yes ☐ No
2.29	Does the device support backups?	☐ Yes ☐ No
	Does this procurement include a backup solution?	☐ Yes ☐ No ☐ N/A
2.30	Does this device include an HL7 interface?	☐ Yes ☐ No
	If yes, what will the HL7 interface be used for?	☐ Orders ☐ Results ☐ Billing (DFT) ☐ ADT ☐ Other: _____
If the requested device does not have an EHRM approved connection or interface to Cerner, completion of the 6550 Appendix A is not required beyond this point. Please sign this document and route it for signature, as appropriate.		
2.31	Does the device have an EHRM approved Cerner interface? *For more information, please reference the approved EHRM interface list and the EHRM IO HTM SharePoint site*	☐ Yes ☐ No
	If no, has an NSR been submitted for interface approval?	☐ Yes ☐ No NSR Number:
	If no, to which security authorization boundary will this device/system be added? *For more information on MedMod zones and MD-LITE, please reference the EHRM IO HTM SharePoint site or contact the EHRM IO HTM team at EHRMIOHTM@va.gov.*	☐ MedMod Zone 6A ☐ MedMod Zone 6B ☐ MD-LITE ☐ Other _____
	If no, what is the proposed EHR connection(s)/integration(s) type(s)? *For additional guidance, please contact the EHRM IO HTM team at EHRMIOHTM@va.gov.*	☐ Openlink (HL7) ☐ Compass Router (DICOM) ☐ EHR Gateway (Non-DICOM Image Routing) ☐ Cerner Connectivity Engine (CCE) ☐ CCE Terminal Server (CCE-TS) ☐ Separate HL7 Interface/Middleware Server ☐ None ☐ Other: _____

Submittal/Approval

Biomedical Engineering *Date*

*Area Manager** *Date*

**Area manager signature only required for client/server medical systems. Please sign within 10 business days of receipt.*

*Information Systems Security Officer*** *Date*

*** Please sign within 5 business days of receipt and return the document to Biomedical Engineering and the Area Manager. If an ERA is required, please submit this form with the ERA package to the Specialized Device Cybersecurity Department (SDSD) to initiate the ERA process.*