NAVAL MEDICAL LOGISTICS COMMAND (NMLC)

Medical Equipment and Logistics Solutions (MELS)
Imaging Informatics Division
693 Neiman Street, Ft. Detrick Maryland 20702

Medical Device Risk Assessment Questionnaire version 3.0

To ascertain security compliance that is in agreement with Federal, DoD, DON and DHA directives and policies, Naval Medical Logistics Command (NMLC) requires the vendor complete the following Medical Device Risk Assessment Questionnaire (MDRA).

All Medical Systems/Devices are required to meet DoD Cybersecurity and NIST Standards. The information provided below will be used to support all stakeholders working to achieve an Authorization Certificate. Failure to meet Cybersecurity requirements, disclose that a system cannot meet Cybersecurity requirements, or failure to meet certification timeframes shall result in Denial of an Authority to Operate (DATO).

The information provided below will be used to identify the technical characteristics of an information technology (IT) based medical system/device, such as data processing capabilities, current security posture, and level of compliance with the Cybersecurity principles of Confidentiality, Integrity, Availability, and Non-Repudiation.

This document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.

BLUE SECTION

ALL FIELDS MUST BE ADDRESSED; THEREFORE NO RESPONSES, N/A, OR REFERENCES TO EXTERNAL DOCUMENTS ARE NOT ACCEPTABLE.

PREPARER IDENTIFICATION INFORMATION	Reset	Print
Date:		
Name:		
Job Title:		
Company:		
Business Address:		
E-Mail Address:		
Phone Number:		
Web page Address:		

SYSTEM IDENTIFICATION	
1.1 Medical Device Name/Title: Provide the naming convention for the system.	
1.1a Medical Device Acronym: Provide the acronym associated with the medical device, if applicable.	
1.1b **Food and Drug Administration (FDA 510K) or Premarket Authorization letter number, if applicable:** Provide the number associated with the medical device, if applicable.	
1.1c Medical Device Functionality Description: System Functional Description – Provide a brief description of the system functions. For example: The ACME Computer Tomography scanner is a radiographic system used in hospitals, clinics, and medical practices. It enables radiographic and tomographic exposures of the whole body including: skull, chest, abdomen, and extremities. The ACME Tomography system converts x-rays to electronic signals.	
1.2 Mode of operation: Select the intended mode of operation of the medical device.	☐ Standalone – Operates in complete isolation and thus does not require the use of networking protocols. ☐ Peer to Peer – Operates in complete isolation but requires the use of networking protocols. ☐ Client/Server – Operates as a distributed application that partitions task or workloads between the service requester (client) and the service provider (server) through the use of networking protocols. ☐ Web-based – Operates as a distributed application that requires the use of a browser to access the primary application. There is no client software installed on the client workstation. ☐ Host-based – Operates as a passive subsystem which requires connection a host computer to produce information. It may require the use of networking protocols. ☐ None of the above – Does not receive, process, store, display information

If none of the capabilities are provided by the proposed medical device described above, completion of the Medical Device Risk Assessment Questionnaire is **NOT** required beyond this point.

SYSTEM IDENTIFICATION	
1.3 Electronic Protected Health Information (ePHI): (Indicate whether the proposed medical device collects, maintains, and/or communicates ePHI. If so, please indicate which items considered ePHI the system processes, either temporarily or permanently). ePHI identifiers are: • Name • Address • Dates of Birth, Admission, Discharge, Death, and all ages over 89 [and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older] • Telephone numbers • Fax number • E-Mail address • Medical Record Number • Health Plan beneficiary number • Account number • Certificate/License number • Any vehicle or other device serial number • Device identifier or serial numbers • Web Uniform Resource Locator (URL) • IP address • Finger or voice prints • Photographic/Radiographic images • Test Results • Physiologic data with identifying characteristics • Biometric data • Personal Financial Data • Any other unique identifying number, characteristic, or code.	Does the system collect, maintain or communicate ePHI? (If yes, list below) ☐ Yes ☐ No In addition to the ePHI question on the left, does the proposed medical device process/store Social Security numbers (SSN) regardless of format/notation? ☐ Yes ☐ No Does the system provide a capability to de-identify private data? ☐ Yes ☐ No
1.4 Department of Defense (DoD)/Defense Health Agency (DHA) Authorization: If known, state whether the proposed medical device has been or is currently undergoing the DoD/DHA Authorization Process (RMF/DIACAP/PIT) and indicate the service sponsoring the authorization (Air Force, Army, Navy).	
1.5 Data Processing Capabilities: Does the proposed medical device perform any of the following data processing functions?	☐ Receive ☐ Process ☐ Store ☐ Route ☐ Display (check all that apply)
1.6 Data Transmitting Mechanisms: Does the proposed medical device perform any of the following data transmitting mechanisms	☐ Generate Hardcopy Reports or Images containing private data ☐ Retrieve private data from removable media ☐ Record private data on removable media ☐ Transmit/receive private data via a wired network connection ☐ Transmit/receive private data via a point-to-point dedicated cable ☐ Import private data through scanning ☐ Unlisted mechanism for importing/exporting, or transmitting of private data (check all that apply)

1.7 Operating System (OS):

Operating System (OS) – Select each and all instances of operating systems used throughout the proposed medical device. Make sure to identify all instances regardless of platform (i.e. server, client, peer, standalone, portable, peripheral end point device), and mode of operation (physical, virtual).

	Microsoft Server Operating Systems	Service Pack
☐	Microsoft Windows Server 2016	
☐	Microsoft Windows Server 2012 R2	
☐	Microsoft Windows Server 2012	
☐	Microsoft Windows Server 2008 R2	
☐	Microsoft Windows Server 2008	
☐	Microsoft Windows Server 2003 R2	
☐	Microsoft Windows Server 2003	
☐	Microsoft Windows Server 2000	
☐	Microsoft Windows NT 4.0 Server	
☐	Microsoft Windows NT 3.51 Server Edition	
☐	Microsoft Windows NT 3.5 Server Edition	
☐	Microsoft Windows NT 3.1 Advanced Server Edition	
	Microsoft Client Operating Systems	**Service Pack**
☐	Microsoft Windows 10 Enterprise	
☐	Microsoft Windows 10 Professional	
☐	Microsoft Windows 10 Enterprise LTSB	
☐	Microsoft Windows 8/8.1	
☐	Microsoft Windows 7 Ultimate	
☐	Microsoft Windows 7 Professional	
☐	Microsoft Windows Vista Ultimate	
☐	Microsoft Windows Vista Business	
☐	Microsoft Windows XP Professional	
☐	Microsoft Windows XP Home	
☐	Microsoft Windows XP Tablet	
☐	Microsoft Windows XP Media Center	
☐	Microsoft Windows 2000 Professional	
☐	Microsoft Windows ME	
☐	Microsoft Windows 98/98 SE	
☐	Microsoft Windows 95	
☐	Microsoft Windows CE 6.0	
☐	Microsoft Windows 2013 Mobile	
☐	Microsoft DOS 6.22/6.0/5.0	

	Microsoft Embedded Operating Systems	Service Pack
☐	Microsoft Windows 10 Mobile	
☐	Microsoft Windows 10 Mobile Enterprise	
☐	Microsoft Windows 10 lo T Core	
☐	Microsoft Windows 8.1 Professional Embedded	
☐	Microsoft Windows 8 Standard Embedded	
☐	Microsoft Windows 8.1 Handheld Embedded	
☐	Microsoft Windows 8.1 Industry Enterprise Embedded	
☐	Microsoft Windows 8.1 Industry Professional Embedded	
☐	Microsoft Windows 7 Ultimate for Embedded Systems	
☐	Microsoft Windows 7 Professional for Embedded Systems	
☐	Microsoft Windows XP Embedded	
☐	Microsoft Windows XP Point of Service	
☐	Microsoft Windows CE 6.0 Embedded	
☐	Windows Embedded Compact 2013	
☐	Windows Embedded Compact 7	
☐	Windows Embedded Handheld 6.5	
☐	Windows Storage Server 2008 Workgroup Embedded	
☐	Windows Storage Server 2008 Standard Embedded	
☐	Windows Storage Server 2008 Enterprise Embedded	
☐	Windows Storage Server 2008 Basic Embedded 32-bit	
☐	Windows Storage Server 2008 Basic Embedded	
☐	Windows Server 2012 R2 for Embedded Systems	
☐	Windows Server 2012 for Embedded Systems	
☐	Microsoft Windows NT Embedded 4.0	
☐	Windows Embedded Standard 2009	
☐	Microsoft Embedded Other	

(SELECT ALL THAT APPLY)

1.7 Operating System (OS) - Continued:

Operating System (OS) – Select each and all instances of operating systems used throughout the proposed medical device. Make sure to identify all instances regardless of platform (i.e. server, client, peer, standalone, portable, peripheral end point device), and mode of operation (physical, virtual).

	LINUX/UNIX based Operating Systems	Version/Kernel
☐	Red Hat	
☐	Fedora	
☐	SUSE Linux Enterprise	
☐	openSUSE Linux	
☐	Debian	
☐	Ubuntu	
☐	BSD	
☐	Knoppix	
☐	Mandriva	
☐	Oracle Solaris	
☐	CentOS	
☐	Google Chromium	
☐	Android OS	
☐	QNX	
☐	Apple OS	
☐	Apple IOS	
☐	Cisco IOS	
☐	Cisco NX	
☐	Juniper JUNOS	
☐	VMware ESX/ESXi, vSphere	
☐	Wind River - VxWorks RTOS	

	Manufacturer Proprietary Operating Systems

1.8 Relational Database Management System (RDMS), if applicable:

Specify title, version, and service pack/release number of each database engine used by the proposed medical device.

	RDBMS Title	Version

1.9 Ports & Protocols:

Note: You may provide the resulting output from a NETSTAT –A command if applicable.

(Ports, Protocols and Services (PPS) – List all Ports, Protocols, and Services used by the proposed medical device. Include for each Port Number: Data Service, Protocol, Purpose, Source and Destination). For example, Hypertext Transport Protocol over Secure Socket Layer (HTTPS/SSL) TCP port 443.

1.10 Antimalware:

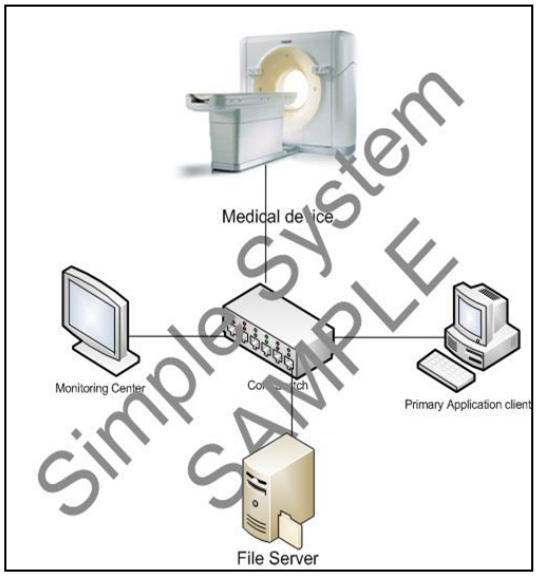
Antimalware – Indicate whether the proposed medical device supports the use of Antimalware applications. If so, indicate which products, including title, version and build number, that have been validated for use with the medical device. For example, Symantec Endpoint Protection version 1.0

SYSTEM IDENTIFICATION	
1.11 Public Internet: Public Internet – Does the proposed medical device require connectivity (permanent, temporary) to the public Internet in order to operate?	
1.12 Operating System (OS) Lifecycle Support: Describe the licensing method of the operating system, including its anticipated End of Life (EOL) date and provisions for Extended support once the operating system is no longer supported by the manufacturer.	
1.13 IPv6 Capability: Is the proposed medical device IPv6 Capable? IPv6 'capable' is defined as a system or product capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to IPv4.	
1.14 Automatic Logoff Does the medical device provide any of the following capabilities to ensure system security if the clinical user walks away without logging out? (If the Operational Use Case makes this a prohibitive process, please provide justification)	☐ Ability to configure the forced reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g. auto-logoff, screen lock, password protected screensaver?) ☐ Ability to configure the length of inactivity time before auto-logoff/screen lock (indicate time [fixed or configurable range] ☐ Ability to manually invoke auto-logoff/screen lock (e.g. via a shortcut key or proximity sensor) (SELECT ALL THAT APPLY)
1.15 DoD Warning Banner Does the medical device provide the capability to implement a customizable warning banner during user login that would enable for display of the DoD Warning Banner?	☐ Yes ☐ No

SYSTEM IDENTIFICATION

1.16a Medical Device Architecture Diagram (simple topology)

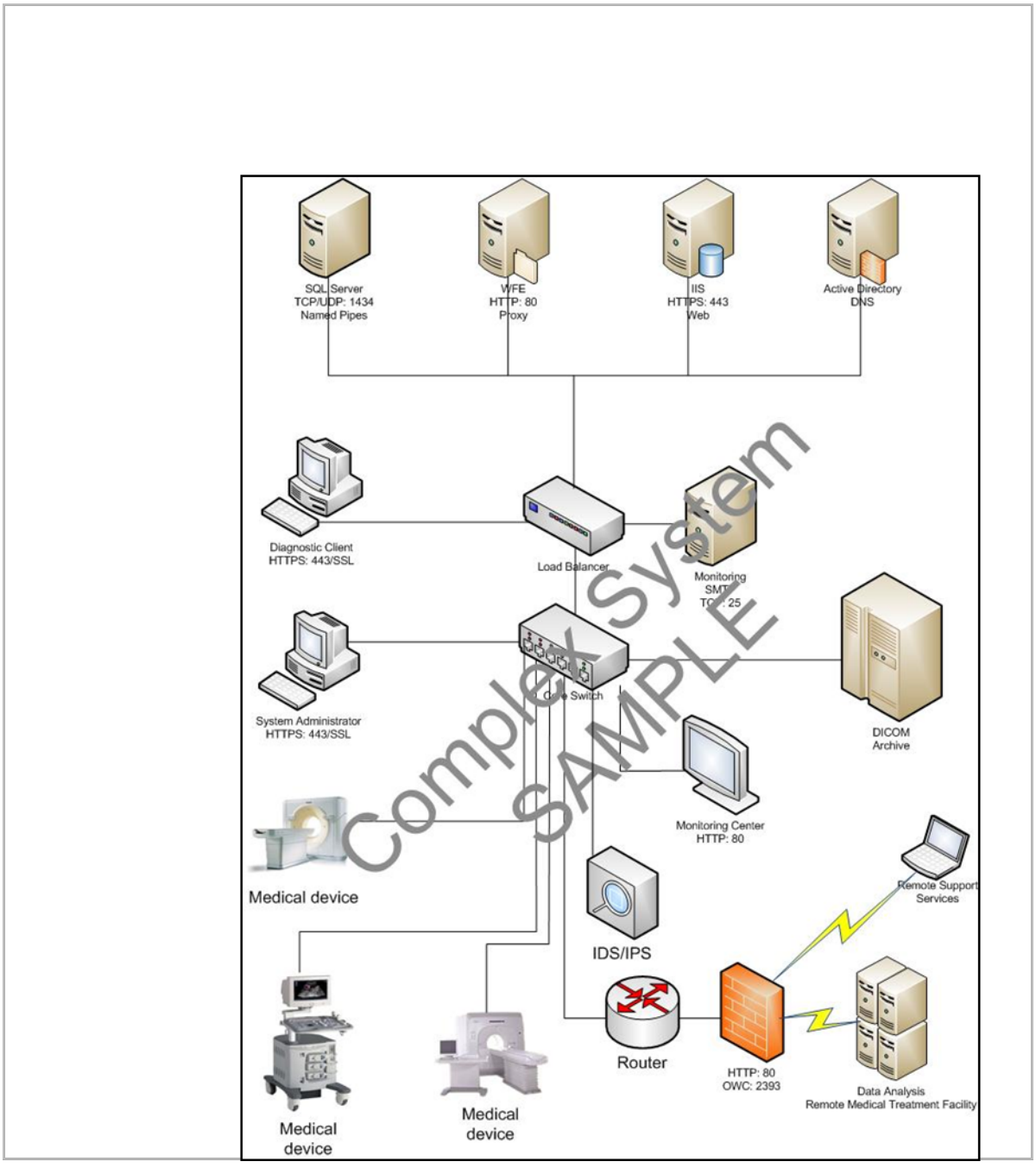
Provide a block diagram depicting all subsystems and components of the proposed medical device as configured in your proposal. Include connection specifications such as: Ethernet Connection, Wireless Connection or Bluetooth Connection The sample diagram shown below may be used as a template for simple topology architectures. You may include an embedded Microsoft Visio diagram with your submission.



SYSTEM IDENTIFICATION

1.16b Medical Device Architecture Diagram (complex topology)

Provide a block diagram depicting all subsystems and components of the proposed medical device as configured in your proposal. The sample diagram shown below may be used as a template for complex topology architectures. You may include an embedded Microsoft Visio diagram with your submission.



GOLD SECTION

MUST BE COMPLETED AND SUBMITTED TO NAVAL MEDICAL LOGISTICS COMMAND (NMLC) WITHIN **10 BUSINESS DAYS** OF AWARD.

THIS SECTION CONTAINS A SERIES OF QUESTIONS REQUIRING A HIGH DEGREE OF FAMILIARITY WITH CONCEPTS AND TERMINOLOGY USED IN INFORMATION TECHNOLOGY. THEREFORE, COMPLETION OF THIS SECTION OF THE MEDICAL DEVICE RISK ASSESSMENT QUESTIONNAIRE BY TECHNICAL PERSONNEL IS REQUIRED. YOU MAY PROVIDE ADDITIONAL PAGES CONTAINING NON-APPLICABLE RESPONSE JUSTIFICATIONS. ALL FIELDS MUST BE ADDRESSED.

GOLD SECTION PREPARER IDENTIFICATION INFORMATION	
Date:	
Name:	
Title:	
Company Name and Address:	
Phone Number:	
E-Mail Address:	

SYSTEM IDENTIFICATION QUESTIONS
2.1 How does the proposed medical system/device ensure Confidentiality? (Describe how the system/device prevents the disclosure of information to unauthorized individuals and/or systems.)
2.2 How does the proposed medical system/device ensure Integrity? (Describe how the system/device prevents the modification of data by unauthorized individuals and/or systems.)
2.3 How does the proposed medical system/device ensure Availability? (Describe how the system/device ensures that the information is available to authorized individuals and/or systems.)
2.4 How does the proposed medical system/device ensure Non-Repudiation? (Describe how the system/device ensures transactions are properly recorded and contain traceable information for auditing purposes.)
2.5 How does the proposed medical system/device protect Data at Rest (DAR)? (Describe how the system/device protects data at rest, for example encryption.)
2.6 How does the proposed medical system/device protect Data in Transit (DIT)? (Describe how the system/device protects data in transit, for example encryption.)
2.7 Does the proposed medical system/device include a test environment instance (physical/virtual)?, if so describe (The purpose of a test environment instance is to allow for the validation and testing of new system components prior to deployment on a production host. These may include software security updates and patches affecting the operating system, primary application, third-party software, database engine, and configuration files). A test environment instance can be physically implemented by using a dedicated (non-production) host, or virtually using a hypervisor.

2.8 OPERATING SYSTEM INVENTORY

Attention: The information required in this section can be generated by using the automated scripts listed in Appendix A. If this information has been collected through the use of automated scripts, completion of this section is not required. Please ensure however that the resulting files are included with your submission and **encrypted**, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.

Title	Version	Expected End of Life (EOL)	Service Pack/Release Level (SP)	32/64-bit Capable	IPv6 Capable

2.9 PRIMARY APPLICATION

2.9a Primary Software Application: Primary Software Application – Provide the title, version, build number and service pack/release number of the primary software application. List all add-ons required by the application, if applicable, such as Virtual Machines, and application software frameworks. For example, ACME Inc. Medical Instrumentation Management System (MIMS) version 3.10 Service Release 2 utilizing Microsoft .NET 3.5 framework.	
2.9b Virtualization: State whether the proposed medical system/device utilizes virtualization technologies. These may include the following: • Operating System virtualization • Application/Workspace • Virtual Desktop Interfaces (VDI) • Storage virtualization • OSI Layer 2/3 switching/routing appliances	
2.9c Web Server: Web Server – if the proposed medical device/system includes one or more web server components, indicate the title and version of the web server engine, for example Microsoft IIS 7.1 or Apache 2.4.10.	
2.9d Browsers: Browsers – If the proposed system requires the use of a browser as the primary application user interface, indicate which versions are supported, for example; Microsoft Internet Explorer 11.	

2.9e Backward Compatibility: Backward compatibility– Describe in detail to what level, does the proposed medical device/system support the operation, interfacing, and exchange of information with regards to previous versions/releases of the same system.	
2.9f Distribution and Installation of Security Updates: Describe the method used to distribute and install security updates, to include both vendor and user responsibilities. If the distribution of Updates/Fixes requires access to a web portal, please provide its URL.	
2.9g Primary Application Licensing method: Describe the licensing method of the primary application, including its anticipated End of Life (EOL) date and provisions for Extended support once the primary application **is no longer supported by the manufacturer**. You may include the anticipated release dates of future versions of the same application if known.	
2.9h Network Addressing/Data Communication Protocols: Network Addressing/Data communication protocol customization: Describe components of the system, if any which rely on the use of TCP/IP addresses and Ports that are **hardcoded and cannot be modified** without a complete rewrite of the application software.	
2.9i Network Time Protocol (NTP): State whether the proposed medical system/device requires the use of a built-in Network Time Protocol source. If so, indicate if this setting can be permanently disabled so as to receive NTP information from the Local Authoritative NTP host provided by the hosting enclave over TCP/UDP port 123.	
2.9j Database Engine: Databases (DB) – List all instances of Database engines including Relational Database Management Systems (RDBMS), and/or flat file based. Include Database title, version, Service Pack/Release. For example, Microsoft SQL Server 2005 Service Pack 2. Describe database authentication method, for example; SQL authentication/Active Directory Integrated authentication, or Mixed Mode authentication.	
2.9k DNS Realm/Domain Integration: If the proposed medical system/device, per design specifications, requires the exchange of data using the TCP/IP protocol, can the system integrate with a DNS Realm/Domain using the LDAP protocol? State whether all or some instances of IP addressable hosts can support this integration. For example; Application Server integrates with Microsoft Active Directory.	
2.9l Automation support: Does the medical system/device support the creation/customization of scripts designed to automate frequent tasks?	

2.9m Compilers on production systems: State whether the proposed medical system/device includes source code compilers/interpreters on production systems and whether they can be removed without affecting the operation of the system. Examples of compilers are: Msc.exe, msvc.exe, Python.exe, javac.exe, Lcc-win32.exe, Microsoft SQL Studio, Microsoft Visual Studio, etc.	
2.9n Administrator Account: State whether the proposed medical system/device requires the use of the built-in "Administrator" (Microsoft Windows) or "root" (UNIX/Linux) accounts to provide authentication to either users and/or services. If so, state whether the medical system/device supports the renaming of these accounts without disrupting its functionality. You may also state whether the authentication of services can be assigned to accounts other than Administrator and/or root.	
2.9o Default Passwords State whether default password can be changed during or prior to installation and identify which accounts have default passwords that can be changed and those accounts in which default passwords cannot be changed.	
2.9p Shared User IDs State whether the system requires a shared user ID and provide the use-case supporting the necessity of a shared user ID.	
2.9q Unused Accounts Are all accounts, which are not required for the intended use of the device disabled or deleted for both users and applications?	
2.9r User interface protection: Describe how the system/device protects direct access to the Operating System interface by unauthorized users.	
2.9s User Privilege Levels Describe how users can be assigned different privilege levels within an application based upon roles.	
2.9t Unrestricted Administrative Account Describe the conditions, if any, in which the device owner or operator has the ability to obtain unrestricted administration privileges (e.g. access operating system or application via local root or admin account).	
2.9u Software Installation Can software or hardware not authorized by the device manufacturer be installed on the device without use of tools?	

2.9v Other platforms supported: Describe whether the primary application is commercially available for other platforms (Mac, Linux, Solaris, Android).	
2.9w Mobile Code: Describe whether the proposed medical system/device uses mobile code technologies. If so, state which technologies are used and if the mobile code can be signed with DoD approved PKI.	
2.9x OS/DB/WEB Server/Application separation: Describe whether the proposed medical system/device supports the physical or logical separation of the Primary Application and the Database Engine, if applicable. Physical separation is accomplished through the utilization of separate disk drives, whereas logical separation is accomplished through the use of separate disk volumes implemented on a single disk drive.	
2.9y Instant Messaging: Does the proposed medical system/device support any type of Instant Messaging (IM), if so describe.	
2.9z Network Resources & Shares (SMB/CIFS, NFS, and AFP): Upon connecting to the Local Area Network, does the medical system/device make its file system available to other systems? If so, please indicate their purpose, default ACL/permissions, and access method (for example, UNC)	
2.9aa SHA-256 Cryptographic & Hash Algorithm support: If applicable, state whether the proposed medical system/device supports the use of SHA-256 Cryptographic and Hash algorithms in support of functions such as - Crypto Logon, reading digitally signed e-mail messages, digitally signing/encrypting data, and client-side PKI based authentication to web-based hosts.	
2.9ab Other Cryptographic & Hash Algorithm Support: Please annotate the non SHA-256 Cryptographic and Hash Algorithms that the medical device uses.	
2.9ac Security Capability Reconfiguration Describe how the device owner/operator reconfigures product security capabilities (e.g. implement system configuration changes and software patches). If the device owner/operator cannot reconfigure product security capabilities, provide statement explaining the mitigation. (e.g., The device owner or operator does not receive administration permissions that enable for system security changes).	

2.10 APPLICATION DEVELOPMENT ENVIRONMENT (non-web based applications)	
Programming Language(s)	Target Applications

2.11 APPLICATION DEVELOPMENT ENVIRONMENT – (web browser based applications)	
Programming Language(s)	Target Applications

2.12 MEDICAL DEVICE HARDWARE/FIRMWARE INVENTORY		
Attention: The information required in this section can be generated by using the scripts and commands listed in Appendix A. If this information has been collected through the use of automation, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (**https://safe.amrdec.army.mil/safe/Welcome.aspx**). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.		
Title	Version	Purpose

2.13 MEDICAL DEVICE SOFTWARE INVENTORY		
Attention: The information required in this section can be generated by using the scripts and commands listed in Appendix A. If this information has been collected through the use of automation, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.		
Title	Version	Purpose

2.14 PHYSICAL/LOGICAL TOPOLOGY DIAGRAM WITH EXTERNAL INTERFACES AND DATA FLOW

Provide a block diagram depicting all interfaces used by the proposed medical system/device. Ensure that for each interface the direction of data flow is clearly shown. Diagram must also clearly show Ports, Protocols, and Services (PPS) for each connection. You may include an embedded Microsoft Visio diagram with your submission.

2.15 ESSENTIAL SERVICES

Attention: The information required in this section can be generated by using the automated scripts listed in Appendix A. If this information has been collected through the use of automated scripts, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.

Attention: The information required in this section can be generated by using the automated scripts listed in Appendix A. If this information has been collected through the use of automated scripts, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.

Title	Authentication	Purpose

2.16 ESSENTIAL PORTS/PROTOCOLS (Indicate whether port tunneling is used)

Attention: The information required in this section can be generated by using the automated scripts listed in Appendix A. If this information has been collected through the use of automated scripts, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.

Port	Protocol	Purpose	Source	Destination	Purpose

2.17 ESSENTIAL PROCESSESS

Attention: The information required in this section can be generated by using the automated scripts listed in Appendix A. If this information has been collected through the use of automated scripts, completion of this section is not required. Please ensure however that the resulting files are included with your submission and encrypted, as an option you can use the AMRDEC SAFE Site (https://safe.amrdec.army.mil/safe/Welcome.aspx). Please ensure that the Require CAC for Pick-up (all recipients will need to log in with a CAC to download file(s)) option is enabled.

Name	Object	Purpose

2.18 FILE SYSTEM

List all **external** interfaces that support file systems (USB, IEEE1394, SD, SIM). Do not include software license/activation tokens.

System	Purpose	Required?

2.19 FILE SYSTEM

Does the system allow the implementation of file-level access controls? (e.g. NTFS, ext3, ext4, XFS)

2.20 GROUP POLICY OBJECTS (GPO) MICROSOFT WINDOWS OPERATING SYSTEMS ONLY:

Group Policy Objects – applies to Microsoft Operating Systems only.
Describe whether the proposed Microsoft Windows based medical system/device can accept Domain level issued Group Policy Objects without negatively impacting the confidentiality, integrity and availability of the system upon joining the production Domain.

Group Policy Object (GPO) Rule:	**Supported?**
Minimum password length of 15 characters	
Password must meet DoD complexity requirements (case sensitive, 15-characters, lower, upper, numeric, alphabetic, and special characters)	
Store passwords using reversible encryption	
Audit account management – Success, Failure	
Audit directory service access – Success, Failure	
Audit object access – Success, Failure	
Audit policy change – Success, Failure	
Allow users to select new root certification authorities (CAs) to trust	
Client computers can trust the following certificate stores – Third Party Root CAs and Enterprise Root CAs	
Perform certificate-based authentication of users and computers, CAs must meet the following criteria – Registered in AD only	

2.20 GROUP POLICY OBJECTS (GPO) MICROSOFT WINDOWS OPERATING SYSTEMS ONLY: Group Policy Objects – applies to Microsoft Operating Systems only. Describe whether the proposed Microsoft Windows based medical system/device can accept Domain level issued Group Policy Objects without negatively impacting the confidentiality, integrity and availability of the system upon joining the production Domain.	
Group Policy Object (GPO) Rule:	**Supported?**
Enforce password history – 24 passwords remembered	
Maximum password age – 60 days	
Minimum password age – 1 day	
Account lockout duration – 0 minutes	
Account lockout threshold – 3 invalid logon attempts	
Reset account lockout counter after – 60 minutes	
Enforce user logon restrictions – Enabled	
Maximum lifetime for service ticket – 600 minutes	
Maximum lifetime for user ticket – 10 hours	
Maximum lifetime for user ticket renewal – 7 days	
Maximum tolerance for computer clock synchronization – 5 minutes	
Enable computer and user accounts to be trusted for delegation – BUILTIN\Administrators	
Network security: Do not store LAN Manager hash value on next password change – Enabled	
Network security: Configure encryption types allowed for Kerberos - Enabled	
Automatic certificate management – Disabled	
Allow users to select new root certification authorities (CAs) to trust – Enabled	
Client computers can trust the following certificate stores – Third-Party Root and Enterprise Root Certification Authorities	
To perform certificate-based authentication of users and computers, CAs must meet the following criteria – Registered in Active Directory	

2.21 IS THE SYSTEM EQUIPED WITH INTELLIGENT PLATFORM MANAGEMENT INTERFACES (IPMI)? IPMI technology allows out of band management of computer systems bypassing the Operating System. If so describe its intended purpose and list specific services required to support the system. Indicate whether IPMI traffic supports encryption of Data in Transit, to and from the Baseboard Management Controller (BMC), and whether “cipher 0” can be disabled.

2.22 AUTHENTICATION Does the proposed medical system/device support any of the following?	Supported?
DoD Password complexity rules (case sensitive, 15-characters, lower, upper, numeric, alphabetic, and special characters)	
Password History/Aging (90 days)	
Operating System services that utilize anonymous access (e.g. Service account not able to be traced to an individual)	

Biometrics	
Public Key Infrastructure (PKI) using X.509 certificates	
Remote Access authentication	
Certificates/Tokens	
Configuration of user lock-out after a certain number of unsuccessful logon attempts	

2.23 AUDITING Does the proposed medical system/device supports any of the following?	Supported?
Audit logs	
Customizable audit levels	
Retention settings for system logs	
Audit logs protection from deletion	
Audit reduction capability that supports on-demand audit review and analysis?	
Audit reduction capability that supports on-demand reporting requirements?	
Audit reduction capability that supports after-the-fact investigations of security incidents?	
Audit reduction capability that does not alter original content or time ordering of audit records?	
Are audit trail events date/time stamped?	
Are audit trail events date/time stamped that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)?	
Can audit trail events include source/destination IP information?	
Can audit trail events include protocols?	
Can audit trail events include User ID information?	
Can audit trail events include changes to Administrator account information?	
Can audit trail events include login/logout information?	
Can audit trail events include the display/presentation of data?	
Can audit trail events include the creation, modification and deletion of data?	
Can audit trail events include the import and export of data to and from removable media?	
Can audit trail events include the receipt and transmission of data with external (e.g. network) connections?	
Can audit trail events include Remote Service activity?	
Can audit trail events include the logging of the execution of privileged functions?	

2.24 BIOS FIRMWARE (FW)	Supported?
Is the BIOS Firmware configuration password-protected?	
Is there a BIOS Firmware master override provided by the vendor?	
Can the device be restricted from booting from uncontrolled or removable media through the BIOS?	

2.25 REMOTE ACCESS The software that provides the remote access capability must be included in the Software Inventory, 2.13. Examples of remote desktop software applications are Microsoft Remote Desktop (MSRDP) and Secure Shell (SSH)	Supported?
Does the device how the ability to be serviced remotely if appropriate B2B agreements are established?	
Can the device be configured to require the local use to accept or initiate remote access?	
Does the device provide an explicit indication of use to users physically present at collaborative computing devices?	

2.26 VULNERABILITY MANAGEMENT Provide a summary describing the plan for providing validated software updates and patches throughout the life cycle of the medical device. The summary should describe how the security patch is validated and then installed (e.g. remote installation by the vendor or distribution by the vendor for biomedical personnel at the healthcare organization to install. The vendor should also specify the frequency of product updates. Note: A vendor may answer this question by providing the product's or organization's vulnerability management plan submitted to the FDA as part of the Premarket Submission Content, if the plan addresses validation, distribution, and installation of security updates.

2.27 ANTIVIRUS/ANTIMALWARE	Supported?
Antivirus/Antimalware recommended best practices (if available) **List items which should be excluded from scanning.*	
Antivirus/Antimalware Heuristics scanning supported?	
Does the system provide notification of malware detection in the device user interface or through other mechanism (describe)?	
Does the system automatically update malicious code protection mechanisms?	
Can only manufacturer-authorized persons repair systems when malware has been detected?	

2.28 DATA AT REST (DAR)	Supported?
Is the encryption algorithm NIST FIPS 140.2 compliant?	
DAR Encryption products and versions validated by the manufacturer	
DAR Encryption recommended best practices **Provide technical recommendations that address the protection mechanisms of data at rest.*	
DAR Removable Media **Does the system/device provide encryption of portable media.*	
Backup Encryption supported algorithms (3DES/AES/RC4/Other)	

2.29 DATA IN TRANSIT (DIT)	Supported?
Is the encryption algorithm NIST FIPS 140.2 compliant?	
DIT Encryption technologies and versions validated by the manufacturer	
DIT Encryption recommended best practices * Provide technical recommendations that address the protection mechanisms of data in transit.	

2.30 AVAILABILITY	Supported?
Availability Position Paper on file system redundancy (if available)	
Availability products and versions validated	
Availability recommended best practices (if available) **Provide technical recommendations that address data availability.*	

2.31 IPv6 - IPv6 capability – Indicate whether the following software components of the proposed medical system/device are capable of sending/receiving TCP/IP version 6 datagrams:	Supported?
Is the **Operating System** capable of transmitting/receiving TCP/IP version 6 Datagrams?	
Is the **Primary Application** capable of transmitting/receiving TCP/IP version 6 Datagrams?	
Is the **Database Engine** capable of transmitting/receiving TCP/IP version 6 Datagrams? (if applicable)	

2.32 IPv6 – COMPLIANCE DOCUMENTATION
• If the system/device is natively capable of exchanging data in the three areas listed above, provide letter of compliance. • If the system supports TCP/IP version 6 through the use of hardware/software based TCP/IPv6 transformers, please describe the technical characteristics and methodology employed to achieve IPv4/IPv6 interoperability, along with technical considerations regarding latency, overhead and redundancy. This is particularly important when describing systems that are considered Real Time, and/or High Availability (HA). • If the proposed medical system/device does not currently support IPv6 data communications, please provide a letter of commitment to upgrade to IPv6, including milestones (in company letterhead from the company's vice president or equivalent).

2.33 HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS)	Supported?
Does the proposed medical system/device support the use of a host based Intrusion Prevention System (IPS)?	

2.34 HOST BASED SECURITY SYSTEM (McAfee HBSS)
Host Based Security System – Describe whether the proposed system supports the installation and operation of a Host Based Security System. A Host Based Security System is a commercial software based application specifically designed to protect and maintain the security baseline of a system. It actively monitors, detects and counters against known cyber threats. Host Based Security Systems are managed by local administrators and are configured to address known exploit traffic using an Intrusion Prevention System (IPS) and host firewall. If the proposed medical system/device has been evaluated against a Host Based Security Systems, provide application title, version, and modules used to conduct its evaluation. If false positives were recorded during evaluation use the following section to list all known instances including the process identifiers and their primary purpose. Example: McAfee EndPoint Security, version 1.0.0.

2.35 INTRUSION DETECTION/PREVENTION SYSTEM – FALSE POSITIVES Describe processes likely to create false-positive alerts
Intrusion Detection/Intrusion Prevention Systems – List all processes known to generate false IPS/IDS false positives. For example: spoolsv.exe incorrectly detected as Backdoor. Ciadoor.B, Hacktool.Privshell or VBS.Massscal.Worm malware.

2.36 MEDICAL SYSTEM/DEVICE RECOVERY/LOSS
Applies to laptops, tablets, and portables only.

Accidental loss – Describe whether the proposed medical system/device portable components support remote wipe and/or geo tracking services in the event of accidental loss, theft, misplacement.

2.37 SYSTEM BACK-UP

Provide a description of the back-up procedures. If the back-up procedures are annotated in a manual that the vendor is providing in response to the solicitation, the vendor may reference the manual. If the system provides the capability to send back-ups to a remote system, please describe the type of encryption used to encrypt a back-up and type of encryption utilized if the back-up is sent to a remote system.

2.38 SYSTEM RECOVERY

Provide detailed information on how the product can be restored back to operation in the event of a system failure and the expected timelines.

2.39 SECURE SHUTDOWN

Describe how The system maintains a secure state during shutdown and restart processes; meaning:
- No object reuse occurs that could accidentally compromise the confidentiality of the system data
- Access to the system cannot be gained by unauthorized personnel
- Unauthorized access to system resources cannot be gained by authorized system users
- Shutdown and restart of the system will not cause harm to the patient, if it occurs during a procedure.
- Data files are not corrupted in the event of an unscheduled shut down.

2.40 MEDICAL SYSTEM/DEVICE STANDARDS CONFORMANCE STATEMENTS
For example IHE, DICOM

Conformance Statements - List all conformance statements associated with the system/device. Please provide proof of certification. For example, DICOM, IHE, MDS2.

2.41 SYSTEM USER DESCRIPTIONS Enter 'Individual Account' into Account Name for user accounts that are tied to specific end users. Example Roles: Role Medical technologist, field service engineer, physician, System Administrator		
Role	Account Name	Minimum Access Level (non-privileged, privileged, administrator/root)

2.42 WIRELESS (IEEE 802.11)	
State whether the medical system/device employs any form of wireless communication, either standards-based and/or proprietary to facilitate the transmission/reception of data between system components and/or other systems?	Supported?
Does the system employ wireless communication?	
Wireless Mode of Operation ad hoc?	
Wireless Mode of Operation infrastructure?	

2.43 WIRELESS – IEEE 802.15 BLUETOOTH (Wireless Personal Area Network – WPAN)			
Frequency (GHz)	Modulation	Throughput (Mbps)	Range (ft.) (indoor/outdoor)

2.44 WIRELESS – IEEE 802.15 ZigBee			
Frequency (GHz)	Modulation	Throughput (Mbps)	Range (ft.) (indoor/outdoor)

2.45 WIRELESS – IEEE 802.11 (a/b/g/n)			
Frequency (GHz)	Modulation (FHSS/OFDM/DSSS/CCK)	Throughput (Mbps)	Range (ft.) (indoor/outdoor)

2.46 WIRELESS – OTHER – ULTRA WIDE BAND (UWB), IEEE 802.16 WiMAX, IR/MICROWAVE, ULTRASOUND, RADIO (VHF/UHF)			
Frequency (GHz)	Modulation	Throughput (Mbps)	Range (ft.) (indoor/outdoor)

2.47 OTHER	
Power Requirements (Voltage/Amps):	
Weight (lbs.)	
Environmental Specifications:	

2.48 PHYSICAL SAFEGUARDS	Supported?
Does the system include a physical locking anti-tampering sensor mechanism?	
Does the system expose data interfaces, such as USB/IEEE 1394 which could be used to bypass the Operating System?	

2.49 SYSTEM AND APPLICATION HARDENING	Supported?
Does the system include a physical locking anti-tampering sensor mechanism?	
Does the system expose data interfaces, such as USB/IEEE 1394 which could be used to bypass the Operating System?	

2.50 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – PRODUCT MANAGER (PM)		
Name	Phone	E-Mail

2.51 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – APPLICATION/NETWORK ENGINEER		
Name	Phone	E-Mail

2.52 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – SECURITY MANAGER		
Name	Phone	E-Mail

2.53 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – INCIDENT REPORTING		
Name	Phone	E-Mail

APPENDIX A

To obtain a detailed list of various components of operating systems, including firmware information, follow the procedure outlined below. Instructions are provided for Microsoft Windows, Linux (including the most common distributions), and VMware. Please ensure that the output produced by the various utilities and commands is captured using plain text formatted (.txt) files. For consistency, you may name these files using the hostname of the device and the data they contain; for example:

"meddev1-os-info.txt"

And

"meddev1-sw-info.txt"

Operating System Inventory

Microsoft Windows operating systems (all currently supported versions)

1. Using local administrative rights, access the Microsoft Windows desktop interface
2. From the command prompt, launch the **MSINFO32.EXE** utility
3. Select File + Export from the main menu
4. Save the file in text format

LINUX based medical systems

1. Access the root prompt
2. Enter the **uname –a > filename** or **uname –mrs > hostname-os-info.txt** commands, where filename denotes the output file
3. You may also obtain similar information by using **dmesg > hostname-os-info.txt** where filename denotes the output file

VMWare based medical systems

1. Access the VMWare service console
2. At the root prompt, enter **vmware –vl**
3. You may redirect the output of the above command as follows: **vmware –vl > hostname-os-info.txt**

Software Inventory

Microsoft Windows based medical devices (all currently supported versions)

1. Access the Microsoft Windows desktop interface
2. Run the PowerShell command interface (Start + Accessories + System Tools + PowerShell)
3. At the PowerShell prompt, type **wmic**
4. At the WMIC prompt, enter **/output:c:\hostname-sw-info.txt product get name,version** and notice that the spacing and punctuation has to be exactly as shown above, for instance no spaces between "name,version"

LINUX based medical devices

1. CentOS – At the root prompt, type the following command: **rpm –qa | less > hostname-sw-info.txt**
2. Debian - At the root prompt, type the following command: **dkpg –get-selections > hostname-sw-info.txt**
3. Ubuntu - At the root prompt, type the following command: **sudo dpkg—get-selections > hostname-sw-info.txt**
4. Free BSD - At the root prompt, type the following command: **pkg_version | less > hostname-sw-info.txt**
5. OpenBSD - At the root prompt, type the following command: **pkg_version | less > hostname-sw-info.txt**

Services running on LINUX based medical devices

At the root prompt, enter **service –list –all > hostname-proc-info.txt**

Active ports and protocols running on a LINUX/Microsoft Windows based medical device

At the root/command prompt, enter **netstat –a > hostname-ports-info.txt**

Active processes running on a LINUX based medical device

At the root prompt, enter **ps –a > hostname-procs-info.txt**

DO NOT COMPLETE ANYTHING BEYOND THIS POINT

IDENTIFICATION INFORMATION	
ACN:	
TDP:	
MDRAQ Serial Number:	
CE POC:	
Contracting POC:	
Blue Section Reviewed By:	
Gold Section Reviewed By:	
Final Disposition:	
Overall Risk Level:	
PMO Authorization Path Recommendation:	

TECHNICAL RECOMMENDATION