



**Naval Medical Logistics Command (NMLC)  
Medical Device Risk Assessment (MDRA)**

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

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

**PREPARER IDENTIFICATION INFORMATION**

Date:		
Name:		
Title:		
Company Name and Address:		
Phone Number:		
E-Mail Address:		

**SYSTEM IDENTIFICATION**

<p><b>1.1 Medical Device Name/Title:</b> (System Name – Provide the naming convention for the system name and associated acronym (if any). For example “ACME Computed Tomography Scanner model 200E (US200)”</p>		
<p><b>1.1a Medical Device Acronym:</b> Provide the commercial acronym associated with the proposed medical device, if applicable.</p>		
<p><b>1.1b Food and Drug Administration (FDA 510K)</b> Premarket Authorization letter number, if applicable.</p>		
<p><b>1.2 Medical Device Description:</b> (System Description – Provide a brief description of the system architecture). For example: The ACME Computer Tomography scanner is a radiographic system used on hospitals, clinics, and medical practices. It enables radiographic and tomographic exposures of the whole body including: skull, chest, abdomen, and extremities. The ACME Computer Tomography system converts x-rays to electronic signals.</p>		

**SYSTEM IDENTIFICATION**

**1.2a 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, exact age if over 89
- 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 images
- 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

**1.3 Department of Defense (DoD) Certification & Accreditation Status:**

(Certification & Accreditation (C&A) Status – If known, state whether the proposed medical device has been or is currently undergoing the DoD Certification & Accreditation Process (DIACAP/PIT/CON)

**1.4 Data Processing Capabilities:**

(Data processing capabilities – With regards to data processing, does the proposed medical device perform any of the following functions?

Receive  Process  Store  Route  Display  None

*(check all that apply)*

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**

**1.5 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).

**(SELECT ALL THAT APPLY)**

	<b>Microsoft Operating Systems</b>	<b>Service Pack</b>
<input type="checkbox"/>	Microsoft Windows 2012 Server	
<input type="checkbox"/>	Microsoft Windows 2008 R2 Server	
<input type="checkbox"/>	Microsoft Windows 2008 Server	
<input type="checkbox"/>	Microsoft Windows 2003 R2 Server	
<input type="checkbox"/>	Microsoft Windows 2003 Server	
<input type="checkbox"/>	Microsoft Windows 2000 Server	
<input type="checkbox"/>	Microsoft Windows 8/8.1	
<input type="checkbox"/>	Microsoft Windows 7 Ultimate	
<input type="checkbox"/>	Microsoft Windows 7 Professional	
<input type="checkbox"/>	Microsoft Windows Vista Ultimate	
<input type="checkbox"/>	Microsoft Windows Vista Business	
<input type="checkbox"/>	Microsoft Windows XP Professional	
<input type="checkbox"/>	Microsoft Windows XP Home	
<input type="checkbox"/>	Microsoft Windows XP Tablet	
<input type="checkbox"/>	Microsoft Windows XP Media Center	
<input type="checkbox"/>	Microsoft Windows 2000 Professional	
<input type="checkbox"/>	Microsoft Windows ME	
<input type="checkbox"/>	Microsoft Windows 98/98 SE	
<input type="checkbox"/>	Microsoft Windows 95	
<input type="checkbox"/>	Microsoft Windows CE 6.0	
<input type="checkbox"/>	Microsoft Windows 2013 Mobile	
<input type="checkbox"/>	Microsoft DOS 6.22/6.0/5.0	

	<b>Microsoft Embedded Operating Systems</b>	<b>Service Pack</b>
<input type="checkbox"/>	Microsoft Windows 8.1 Professional Embedded	
<input type="checkbox"/>	Microsoft Windows 8 Standard Embedded	
<input type="checkbox"/>	Microsoft Windows 8.1 Handheld Embedded	
<input type="checkbox"/>	Microsoft Windows 8.1 Industry Enterprise Embedded	
<input type="checkbox"/>	Microsoft Windows 8.1 Industry Professional Embedded	
<input type="checkbox"/>	Microsoft Windows 7 Ultimate for Embedded Systems	
<input type="checkbox"/>	Microsoft Windows 7 Professional for Embedded Systems	
<input type="checkbox"/>	Microsoft Windows XP Embedded	
<input type="checkbox"/>	Microsoft Windows XP Point of Service	
<input type="checkbox"/>	Microsoft Windows CE 6.0 Embedded	
<input type="checkbox"/>	Windows Embedded Compact 2013	
<input type="checkbox"/>	Windows Embedded Compact 7	
<input type="checkbox"/>	Windows Embedded Handheld 6.5	
<input type="checkbox"/>	Windows Storage Server 2008 Workgroup Embedded	
<input type="checkbox"/>	Windows Storage Server 2008 Standard Embedded	
<input type="checkbox"/>	Windows Storage Server 2008 Enterprise Embedded	
<input type="checkbox"/>	Windows Storage Server 2008 Basic Embedded 32-bit	
<input type="checkbox"/>	Windows Storage Server 2008 Basic Embedded	
<input type="checkbox"/>	Windows Server 2012 R2 for Embedded Systems	
<input type="checkbox"/>	Windows Server 2012 for Embedded Systems	
<input type="checkbox"/>	Microsoft Windows NT Embedded 4.0	
<input type="checkbox"/>	Windows Embedded Standard 2009	
<input type="checkbox"/>	Microsoft Embedded Other	

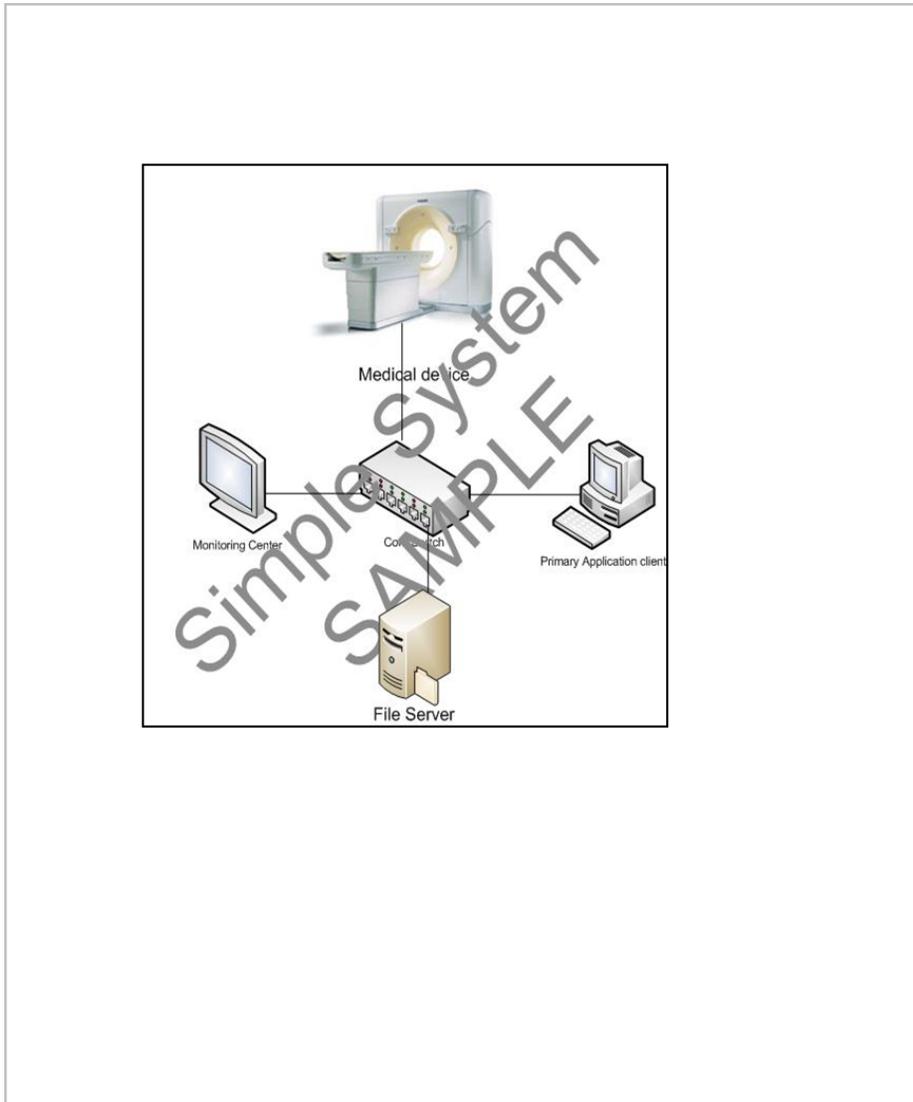
	<b>LINUX/UNIX</b>	<b>Kernel version</b>
<input type="checkbox"/>	Red Hat	
<input type="checkbox"/>	Fedora	
<input type="checkbox"/>	SUSE Linux Enterprise	
<input type="checkbox"/>	openSUSE Linux	
<input type="checkbox"/>	Debian	
<input type="checkbox"/>	Ubuntu	
<input type="checkbox"/>	BSD	
<input type="checkbox"/>	Knoppix	
<input type="checkbox"/>	Mandriva	
<input type="checkbox"/>	Oracle Solaris	
<input type="checkbox"/>	CentOS	
<input type="checkbox"/>	Google Chromium	
<input type="checkbox"/>	Android OS	
<input type="checkbox"/>	QNX	

	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td><input type="checkbox"/></td><td>Apple OS</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>Apple IOS</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>Cisco IOS</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>Cisco NX</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>Juniper JUNOS</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>VMware ESX/ESXi, vSphere</td><td></td></tr> <tr><td><input type="checkbox"/></td><td>Wind River - VxWorks RTOS</td><td></td></tr> <tr> <td></td> <td style="text-align: center;"><b>Manufacturer Proprietary Operating Systems</b></td> <td style="text-align: center;"><b>Version</b></td> </tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> </table>	<input type="checkbox"/>	Apple OS		<input type="checkbox"/>	Apple IOS		<input type="checkbox"/>	Cisco IOS		<input type="checkbox"/>	Cisco NX		<input type="checkbox"/>	Juniper JUNOS		<input type="checkbox"/>	VMware ESX/ESXi, vSphere		<input type="checkbox"/>	Wind River - VxWorks RTOS			<b>Manufacturer Proprietary Operating Systems</b>	<b>Version</b>	<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			
<input type="checkbox"/>	Apple OS																																		
<input type="checkbox"/>	Apple IOS																																		
<input type="checkbox"/>	Cisco IOS																																		
<input type="checkbox"/>	Cisco NX																																		
<input type="checkbox"/>	Juniper JUNOS																																		
<input type="checkbox"/>	VMware ESX/ESXi, vSphere																																		
<input type="checkbox"/>	Wind River - VxWorks RTOS																																		
	<b>Manufacturer Proprietary Operating Systems</b>	<b>Version</b>																																	
<input type="checkbox"/>																																			
<input type="checkbox"/>																																			
<input type="checkbox"/>																																			
<p><b>1.6 Relational Database Management System (RDMS), if applicable:</b> Specify title, version, and service pack/release number of each database engine used by the proposed medical device.</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td></td> <td style="text-align: center;"><b>RDBMS Title</b></td> <td style="text-align: center;"><b>Version</b></td> </tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> </table>		<b>RDBMS Title</b>	<b>Version</b>	<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>																					
	<b>RDBMS Title</b>	<b>Version</b>																																	
<input type="checkbox"/>																																			
<input type="checkbox"/>																																			
<input type="checkbox"/>																																			
<input type="checkbox"/>																																			
<p><b>1.7 Ports &amp; Protocols:</b> (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.</p>																																			
<p><b>1.8 Antimalware:</b> Antimalware – Indicate whether the proposed medical device supports the use of Antimalware applications. If so, indicate which products, including title, version and build number have been validated. For example, Symantec Endpoint Protection version 1.0</p>																																			
<p><b>1.9 Public Internet:</b> Public Internet – Does the proposed medical device require connectivity (permanent, temporary) to the public Internet in order to operate?</p>																																			
<p><b>1.9b Operating System (OS) Lifecycle Support:</b> 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.</p>																																			
<p><b>1.10 IPv6 Capability:</b> 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.</p>																																			

SYSTEM IDENTIFICATION

1.11a Medical Device Architecture Diagram (simple topology)

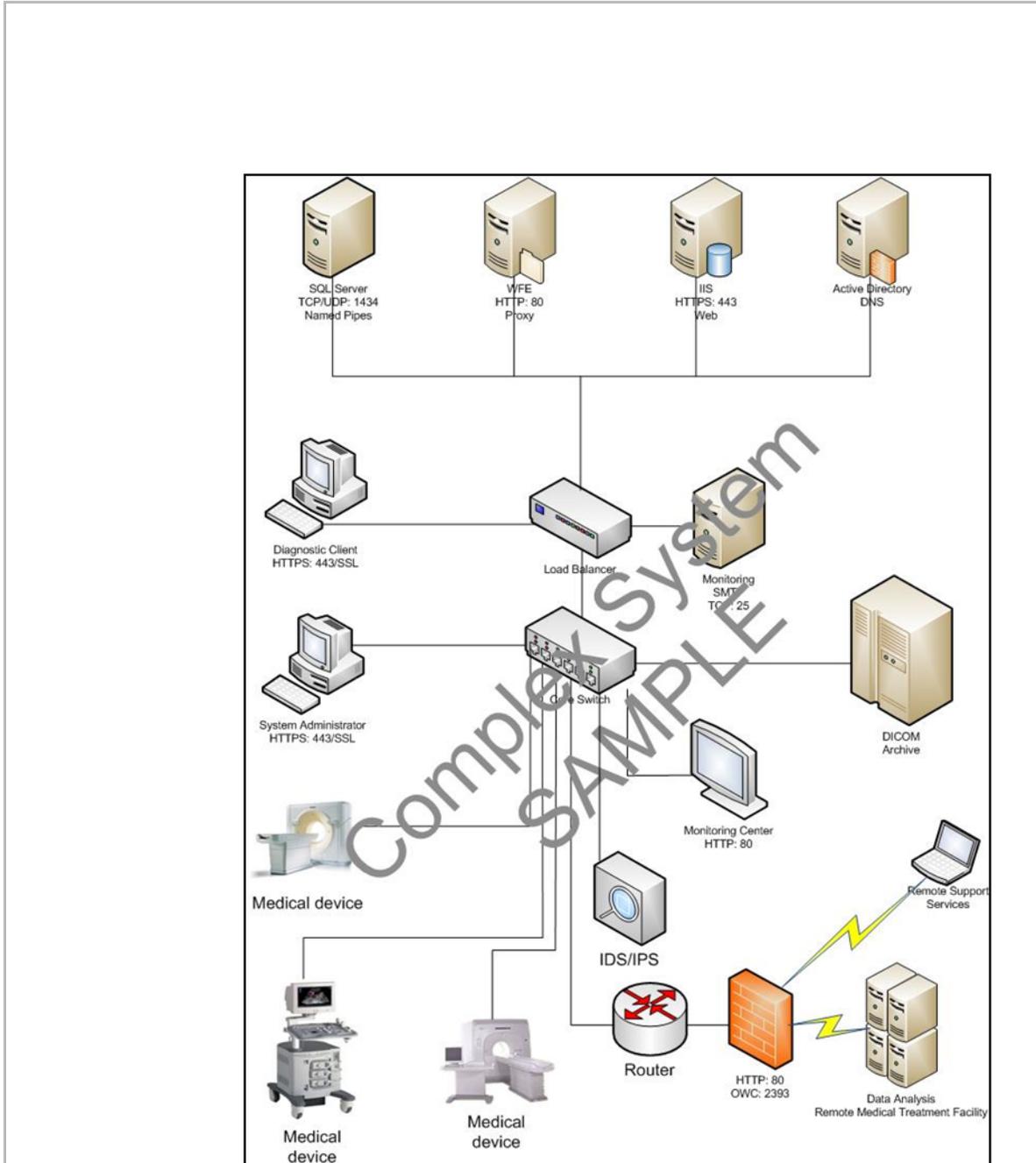
Provide a block diagram depicting all subsystems and components of the proposed medical device as configured in your proposal. The sample diagram shown below may be used as a template for simple topology architectures. You may include an embedded Microsoft Visio diagram with your submission.



SYSTEM IDENTIFICATION

1.11b 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 – THE SECTION THAT FOLLOWS 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.**

**GOLD SECTION PREPARER IDENTIFICATION INFORMATION**

<b>Date:</b>		
<b>Name:</b>		
<b>Title:</b>		
<b>Company Name and Address:</b>		
<b>Phone Number:</b>		
<b>E-Mail Address:</b>		

**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.

--	--

**2.9 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/Welcme.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	

**2.10 PRIMARY APPLICATION**

**2.10a 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.)

--	--

**2.10b 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

--	--

<p><b>2.10c Web Server:</b>                  (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)</p>		
<p><b>2.10c Browsers:</b>                  (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)</p>		
<p><b>2.10d Backward Compatibility:</b>                  (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.)</p>		
<p><b>2.10e Distribution method of Security Updates:</b>                  (If the distribution of Updates/Fixes requires access to a web portal, please provide its URL).</p>		
<p><b>2.10f Primary Application Licensing method:</b>                  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 <b>is no longer supported by the manufacturer</b>. You may include the anticipated release dates of future versions of the same application if known.</p>		
<p><b>2.10g Network Addressing/Data Communication Protocols:</b>                  (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 <b>hardcoded and cannot be modified</b> without a complete rewrite of the application software.)</p>		
<p><b>2.10h Network Time Protocol (NTP):</b>                  State whether the proposed medical system/device requires the use of a <b>built-in</b> 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.</p>		
<p><b>2.10i Database Engine:</b>                  (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.)</p>		

<p><b>2.10j DNS Realm/Domain Integration:</b> (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.)</p>		
<p><b>2.10k Automation support:</b> (Does the medical system/device support the creation/customization of scripts designed to automate frequent tasks?)</p>		
<p><b>2.10l Compilers on production systems:</b> 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.</p>		
<p><b>2.10m Administrator Account:</b> 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.</p>		
<p><b>2.10n User interface protection:</b> (Describe how the system/device protects direct access to the Operating System interface by unauthorized users.)</p>		
<p><b>2.10o Other platforms supported:</b> (Describe whether the primary application is commercially available for other platforms (Mac, Linux, Solaris, Android))</p>		
<p><b>2.10p Mobile Code:</b> (Describe whether the proposed medical system/device uses mobile code technologies. If so, state if all mobile code can be signed with DoD approved PKI.)</p>		
<p><b>2.10q OS/DB/WEB Server/Application separation:</b> (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.</p>		

<b>2.10r Instant Messaging:</b> (Does the proposed medical system/device support any type of Instant Messaging (IM), if so describe.)		
<b>2.10s Network Resources &amp; Shares (SMB/CIFS, NFS, and AFP):</b> (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)		
<b>2.10t SHA-256 Cryptographic &amp; Hash Algorithm support:</b> (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)	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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

2.13 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 <u>not</u> 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 ( <a href="https://safe.amrdec.army.mil/safe/Welcome.aspx" style="color: white;">https://safe.amrdec.army.mil/safe/Welcome.aspx</a> ). 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	

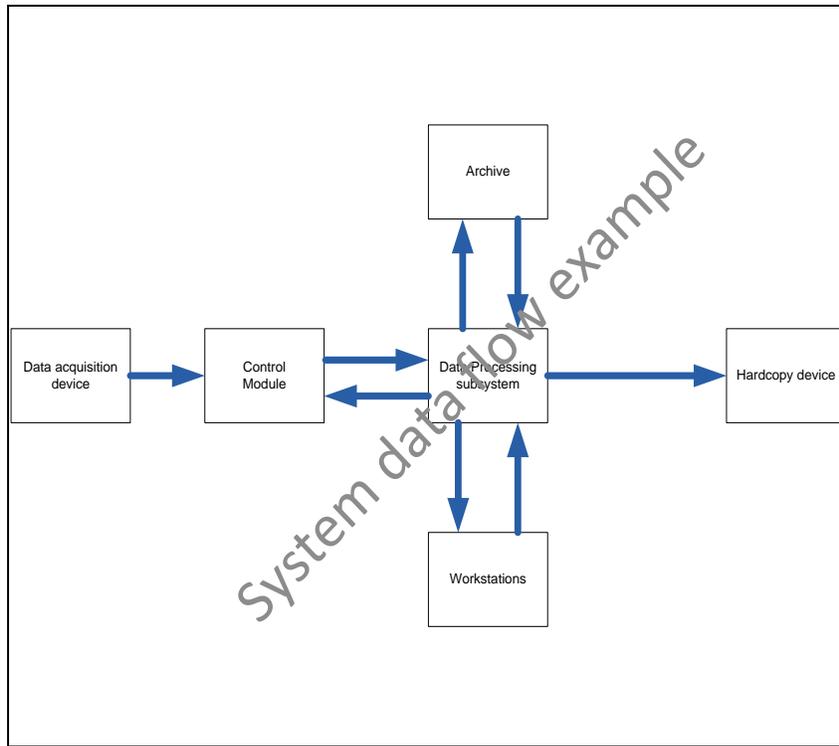
**2.14 MEDICAL DEVICE SOFTWARE INVENTORY**

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	

**2.15 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. You may include an embedded Microsoft Visio diagram with your submission.



**2.16 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.

Name	Authentication	Purpose	

**2.17 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	Data Service	Source	Destination	Purpose	

**2.18 ESSENTIAL PROCESSES**

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	

**2.19 FILE SYSTEM**

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

System	Purpose	Required?	

**2.20 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	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Password must meet complexity requirements	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Store passwords using reversible encryption	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Audit account management – Success, Failure	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Audit directory service access – Success, Failure	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Audit object access – Success, Failure	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Audit policy change – Success, Failure	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Allow users to select new root certification authorities (CAs) to trust	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Client computers can trust the following certificate stores – Third Party Root CAs and Enterprise Root CAs	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Perform certificate-based authentication of users and computers, CAs must meet the following criteria – Registered in AD only	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Enforce password history – 24 passwords remembered	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum password age – 60 days	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Minimum password age – 1 day	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Account lockout duration – 0 minutes	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Account lockout threshold – 3 invalid logon attempts	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Reset account lockout counter after – 60 minutes	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Enforce user logon restrictions – Enabled	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum lifetime for service ticket – 600 minutes	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum lifetime for user ticket – 10 hours	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum lifetime for user ticket renewal – 7 days	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum tolerance for computer clock synchronization – 5 minutes	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Enable computer and user accounts to be trusted for delegation – BUILTIN\Administrators	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Network security: Do not store LAN Manager hash value on next password change – Enabled	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Network security: Configure encryption types allowed for Kerberos - Enabled	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Automatic certificate management – Disabled	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Allow users to select new root certification authorities (CAs) to trust – Enabled	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Client computers can trust the following certificate stores – Third-Party Root and Enterprise Root Certification Authorities	<input type="checkbox"/> Yes <input type="checkbox"/> No	
To perform certificate-based authentication of users and computers, CAs must meet the following criteria – Registered in AD	<input type="checkbox"/> Yes <input type="checkbox"/> No	

**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?)

	Yes	No	
DoD Password complexity rules (case sensitive, 15-characters, lower, upper, numeric, alphabetic, and special characters)	<input type="checkbox"/>	<input type="checkbox"/>	
Password History/Aging (90 days)	<input type="checkbox"/>	<input type="checkbox"/>	
Operating System services that utilize anonymous access	<input type="checkbox"/>	<input type="checkbox"/>	
Biometrics	<input type="checkbox"/>	<input type="checkbox"/>	
Public Key Infrastructure (PKI) using X.509 certificates	<input type="checkbox"/>	<input type="checkbox"/>	
Remote Access authentication	<input type="checkbox"/>	<input type="checkbox"/>	
Certificates/Tokens	<input type="checkbox"/>	<input type="checkbox"/>	

**2.23 AUDITING**  
 (Does the proposed medical system/device support any of the following?)

	Yes	No	
Audit logs	<input type="checkbox"/>	<input type="checkbox"/>	
Customizable audit levels	<input type="checkbox"/>	<input type="checkbox"/>	
Retention settings for system logs	<input type="checkbox"/>	<input type="checkbox"/>	
Audit logs protection from deletion	<input type="checkbox"/>	<input type="checkbox"/>	
Are audit trail events date/time stamped?	<input type="checkbox"/>	<input type="checkbox"/>	
Can audit trail events include source/destination IP information?	<input type="checkbox"/>	<input type="checkbox"/>	
Can audit trail events include protocols?	<input type="checkbox"/>	<input type="checkbox"/>	
Can audit trail events include User ID information?	<input type="checkbox"/>	<input type="checkbox"/>	
Can audit trail events include changes to Administrator account information?	<input type="checkbox"/>	<input type="checkbox"/>	

**2.24 BIOS FIRMWARE (FW)**

	Yes	No	
Is the BIOS Firmware configuration password-protected?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a BIOS Firmware master override provided by the vendor?	<input type="checkbox"/>	<input type="checkbox"/>	

2.25 ANTIVIRUS/ANTIMALWARE			
	Yes	No	
Antivirus/Antimalware recommended best practices (if available) <i>*List items which should be <u>excluded</u> from scanning.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
Antivirus/Antimalware Heuristics scanning supported?	<input type="checkbox"/>	<input type="checkbox"/>	

2.26 DATA AT REST (DAR)			
	Yes	No	
Is the encryption algorithm NIST FIPS 140.2 compliant?	<input type="checkbox"/>	<input type="checkbox"/>	
DAR Encryption products and versions validated by the manufacturer	<input type="checkbox"/>	<input type="checkbox"/>	
DAR Encryption recommended best practices <i>*Provide technical recommendations that address the protection mechanisms of data at rest.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
DAR Removable Media <i>*Does the system/device provide encryption of portable media.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
Backup Encryption supported algorithms (3DES/AES/RC4/Other)	<input type="checkbox"/>	<input type="checkbox"/>	

2.27 DATA IN TRANSIT (DIT)			
	Yes	No	
Is the encryption algorithm NIST FIPS 140.2 compliant?	<input type="checkbox"/>	<input type="checkbox"/>	
DIT Encryption technologies and versions validated by the manufacturer	<input type="checkbox"/>	<input type="checkbox"/>	
DIT Encryption recommended best practices <i>* Provide technical recommendations that address the protection mechanisms of data in transit.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

2.28 AVAILABILITY			
	Yes	No	
Availability Position Paper on file system redundancy (if available)	<input type="checkbox"/>	<input type="checkbox"/>	
Availability products and versions validated	<input type="checkbox"/>	<input type="checkbox"/>	
Availability recommended best practices (if available) <i>*Provide technical recommendations that address data availability.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

2.29 IPv6			
	Yes	No	
(IPv6 capability – Indicate whether the following software components of the proposed medical system/device are capable of sending/receiving TCP/IP version 6 datagrams:	<input type="checkbox"/>	<input type="checkbox"/>	
Is the <b>Operating System</b> capable of transmitting/receiving TCP/IP version 6 Datagrams?	<input type="checkbox"/>	<input type="checkbox"/>	
Is the <b>Primary Application</b> capable of transmitting/receiving TCP/IP version 6 Datagrams?	<input type="checkbox"/>	<input type="checkbox"/>	
Is the <b>Database Engine</b> capable of transmitting/receiving TCP/IP version 6 Datagrams? (if applicable)	<input type="checkbox"/>	<input type="checkbox"/>	

**2.30 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).

**2.31 HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS)**

	Yes	No	
Does the proposed medical system/device support the use of a <u>host based</u> Intrusion Prevention System (IPS)?	<input type="checkbox"/>	<input type="checkbox"/>	

**2.32 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.

**2.33 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.

**2.34 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.

--	--

**2.35 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.


**2.36 SYSTEM USER DESCRIPTIONS**

(For example: Medical technologist, field service engineer, physician)

Role	Minimum Access Level (non-privileged, privileged, administrator/root)	

**2.37 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?

	Yes	No	
Does the system employ wireless communication?	<input type="checkbox"/>	<input type="checkbox"/>	
Wireless Mode of Operation ad hoc?	<input type="checkbox"/>	<input type="checkbox"/>	
Wireless Mode of Operation infrastructure?	<input type="checkbox"/>	<input type="checkbox"/>	

**2.38 WIRELESS – IEEE 802.15 BLUETOOTH**  
(Wireless Personal Area Network – WPAN)

Frequency (GHz)	Modulation	Throughput (Mbps)	Range (ft.) (indoor/outdoor)	

**2.39 WIRELESS – IEEE 802.15 ZigBee**

Frequency (GHz)	Modulation	Throughput (Mbps)	Range (ft.) (indoor/outdoor)	

**2.41 WIRELESS – IEEE 802.15 (a/b/g/n)**

Frequency (GHz)	Modulation (FHSS/OFDM/DSSS/CCK)	Throughput (Mbps)	Range (ft.) (indoor/outdoor)	

**2.42 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)	

**2.43 OTHER**

Power Requirements (Voltage/Amps):		
Weight (lbs.)		
Physical Dimensions (H/W/D):		
Environmental specifications:		

**2.44 PHYSICAL SAFEGUARDS**

	Yes	No	
Does the system include a physical locking anti-tampering sensor mechanism?	<input type="checkbox"/>	<input type="checkbox"/>	
Does the system expose data interfaces, such as USB/IEEE 1394 which could be used to bypass the Operating System?	<input type="checkbox"/>	<input type="checkbox"/>	

**2.45 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – PRODUCT MANAGER (PM)**

Name	Phone	E-Mail

**2.46 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – APPLICATION/NETWORK ENGINEER**

Name	Phone	E-Mail

**2.47 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – SECURITY MANAGER**

Name	Phone	E-Mail

**2.48 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: **dpkg --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**

<b>ACN:</b>	
<b>TDP:</b>	
<b>MDRAQ Serial Number:</b>	
<b>CE POC:</b>	
<b>Contracting POC:</b>	
<b>Blue Section Reviewed By:</b>	
<b>Gold Section Reviewed By:</b>	
<b>Final Disposition:</b>	
<b>Overall Risk Level:</b>	
<b>PMO Authorization Path Recommendation:</b>	

**TECHNICAL RECOMMENDATION**