|  |  |
| --- | --- |
|  | NEW.JPG |

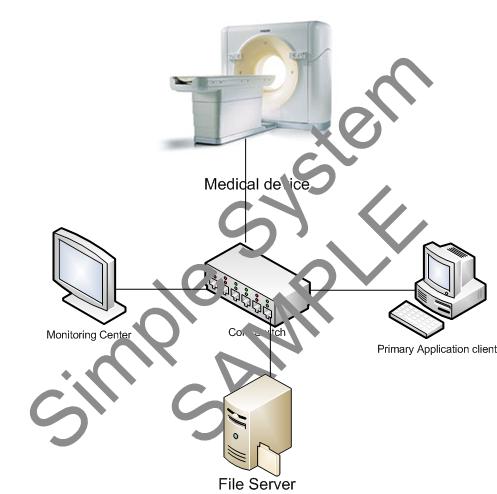
Naval Medical Logistics Command (NMLC)  
Certification & Accreditation (C&A) Initial Technical Questionnaire  
  
Certification and Accreditation (C&A) Process Initial Technical Questionnaire DIACAP/Platform Information Technology Risk Assessment (PIT/PRA)

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

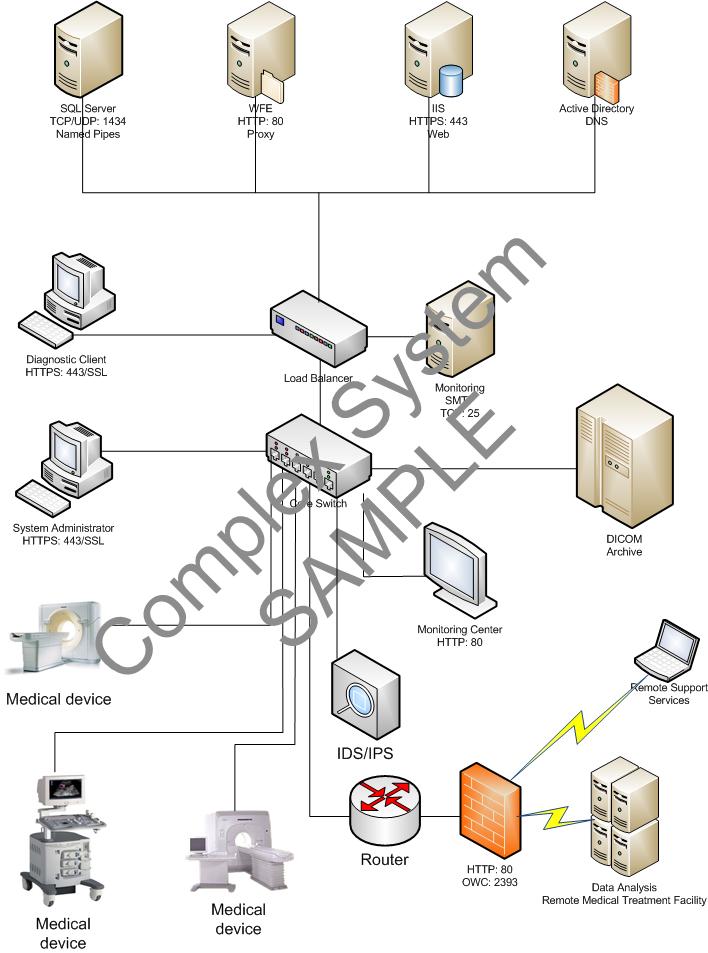
### BLUE SECTION (Shall be submitted with proposal)

| SYSTEM IDENTIFICATION QUESTIONS | | |
| --- | --- | --- |
| 1.1 **System Name:**  (System Name – Provide the naming convention for the system name and associated acronym (if any)) |  |  |
| To help avoid duplicating efforts, if the C&A form has been already been filled out for the same system/device/application please select **YES** and stop. If you have not filled out this form before select **NO** and continue on with finishing the form.   |  |  | | --- | --- | | Yes | No | | | |
| 1.2 **System Description:**  (System Description – Provide a brief high level description of the system architecture) |  |  |
| 1.3 **Certification & Accreditation Status:**  *(Certification & Accreditation (C&A) Status – If known, state whether the system has been or is currently undergoing the DoD Certification & Accreditation Process (DIACAP/PIT/CoN))* |  |  |
| If the above system has already attained Certification & Accreditation, completion of the  remainder of the C&A Initial Technical Questionnaire is **NOT** required. | | |
| 1.4 **Data Processing Capabilities:**  *(Data processing capabilities – With regards to data processing, does the system/device perform any of the following functions (check all that apply))* | |  | | --- | |  | |  | |  | |  | |  | |  |
| If none of the above functions is performed by the system/device described above,  completion of the C&A Initial Technical Questionnaire is **NOT** required. | | |
| 1.5 **Functional Description:**  *(Functional Description – Provide a summary description of the system based on actual capabilities as presently implemented. Include functions that the system should perform, desired interfaces and capabilities associated with the same. Include type of information being processed. Describe core processing and monitoring subsystems, internal and external connections. Describe the system in terms of the acquisition, processing, storing, routing, and presentation of data)* |  |  |
| 1.6 **Operating System/Systems (OS):**  *(Operating System (OS) – List all instances of Operating Systems used throughout the system, including closed source operating systems, open source operating systems, and real-time/ embedded operating systems, including customized versions of the same. State whether each instance is either physical or virtual; include Service Pack/Release level, and 32/64-bit support,). For example, Microsoft Windows XP Service Pack 3* |  |  |
| 1.7 **Primary Application:**  *(Primary Application – Provide primary application title, version. 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.)* |  |  |
| 1.8 **Backward Compatibility:**  *(Backward compatibility– Describe in detail to what level, does the proposed system support the operation, interfacing, and exchange of information with regards to previous versions/releases of the same system.)* |  |  |
| 1.9 **Database Engine:**  *(Databases (DB) – List all instances of Databases 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.)* |  |  |
| 1.10 **Ports & Protocols:**  *(Ports, Protocols and Services (PPS) – List all Ports, Protocols, and Services used throughout the system. Include for each Port Number, Data Service, Protocol, Purpose, Source and Destination. State whether ports are manually configurable or hardcoded. For example, Remote Desktop (RDP) TCP/UDP 3389.)* |  |  |
| 1.11 **Antimalware:**  *(Antimalware (AM) – List all instances of Antimalware applications supported by the system. For example, Symantec Endpoint Protection version 1.0)* |  |  |
| 1.12 **Networking:**  *(Networking – Describe the method of communication employed by the system. Provide details of the communication media (wired, wireless). For example, Wireless Ethernet 802.11n.)* |  |  |
| 1.13 **DNS Realm/Domain Integration:**  *(If the proposed medical system, 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.)* |  |  |
| 1.14 **IPv6 Capability:**  *(IPv6 capability – Describe whether the Operating System and/or Primary Application can operate in an IPv6 networking environment. If system is currently IPv6 capable, provide letter of compliance. If the system will be IPv6 capable in the future, provide letter of commitment to upgrade including milestones (from the company’s Vice President or equivalent))* |  |  |

### System Architecture Diagram (Include all system components; devices, subsystems, ports, servers, routers, firewalls, intrusion prevention/detection systems, etc.)



### System Architecture Diagram (continued) (Include all system components; devices, subsystems, ports, servers, routers, firewalls, intrusion prevention/detection systems, etc.)



### GOLD SECTION (Shall be submitted within seven days of award)

|  |  |
| --- | --- |
| The section that follows contains a series of questions which require a **high degree of familiarity** with concepts and terminology used in both Information Assurance and Information Technology. Therefore completion of the remainder of the C&A Initial Technical Questionnaire by technical personnel is required. Non-Applicable (N/A) responses to any of the items below require a brief explanation.  You may provide additional pages containing Non-Applicable response justifications. | |
| SYSTEM IDENTIFICATION QUESTIONS | |
| 2.1 **How does the proposed 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 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 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 system/device ensure Non-Repudiation?**  *(Describe how the system/device ensures transactions are properly recorded and contains traceable information for auditing purposes.)* | |
|  |  |
| 2.5 **How does the system/device protect Data at Rest?**  *(Describe how the system/device protects data at rest, for example encryption.)* | |
|  |  |
| 2.6 **How does the system/device protect Data in Transit?**  *(Describe how the system/device protects data in transit, for example encryption.)* | |
|  |  |
| 2.7 **Does the system require connectivity to the public internet?, if so describe its purpose** | |
|  |  |
| 2.8 **Does the system provide a test environment? , if so describe** | |
|  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2.9 OPERATING SYSTEM INVENTORY | | | | | | | | |
| Title | Closed Source/  Open Source | Version | RTOS/  Embedded | Virtualization  Support | Service Pack/Release  Level | 32/64-bit  Capable | IPv6  Capable |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.10 **PRIMARY APPLICATION** | | |
| Distribution method of Service Packs/Releases: |  |  |
| Distribution method of Upgrades: |  |  |
| Distribution method of Updates/Fixes: |  |  |
| Licensing method: |  |  |
| 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.)* |  |  |
| Dependencies: *(List all support processes that are essential in real time to the overall functionality of the application.)* |  |  |
| Automation support: *(Does the system/device support the creation of scripts designed to automate frequent tasks.)* |  |  |
| Embedded programming: *(Does the system/device provide access to an Integrated Development Environment (IDE) thus allowing for the customization of software via source code.)* |  |  |
| User interface protection: *(Describe how the system/device protects direct access to the Operating System by unauthorized users.)* |  |  |
| Other platforms supported: *(Describe whether the primary application is commercially available for other platforms (Mac, Linux, Solaris))* |  |  |
| Mobile Code: *(Describe whether the system uses mobile code technologies. If so, state if all mobile code can be signed with DoD approved PKI.)* |  |  |
| OS separation: *(Describe whether the primary application can be physically/logically isolated from the operating system. Examples, separation of volumes, physical disks.)* |  |  |
| Instant Messaging: *(Does the system/device support any type of Instant Messaging (IM), if so describe.)* |  |  |
| Personally Identifiable Information/Protected Health Information (PII/PHI): *(Does the system/device receive/process/store/display Personally Identifiable Information (PII)/Protected Health Information (PHI), if so describe.)* |  |  |

|  |  |  |
| --- | --- | --- |
| 2.11 APPLICATION DEVELOPMENT ENVIRONMENT | | |
| Programming Languages(s) | Target Applications |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.12 APPLICATION DEVELOPMENT ENVIRONMENT – BROWSER BASED | | |
| Programming Languages(s) | Target Applications |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.13 SERVER HARDWARE INVENTORY | | | | |
| Title | Version | Purpose | Common Criteria Evaluation Status |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.14 SERVER SOFTWARE INVENTORY | | | | |
| Title | Version | Purpose | Common Criteria Evaluation Status |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.15 SERVER FIRMWARE INVENTORY | | | | |
| Asset | Manufacturer | Version | Access Control |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.16 CLIENT HARDWARE INVENTORY | | | | |
| Asset | Manufacturer | Model | Purpose |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.17 CLIENT SOFTWARE INVENTORY | | | | |
| Asset | Manufacturer | Model | Purpose |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.18 CLIENT FIRMWARE INVENTORY | | | | |
| Asset | Manufacturer | Model | Access Control |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| 2.19 PHYSICAL/LOGICAL TOPOLOGY DIAGRAM WITH EXTERNAL INTERFACES AND DATA FLOW |



|  |  |  |  |
| --- | --- | --- | --- |
| 2.20 ESSENTIAL SERVICES | | | |
| Name | Authentication | Purpose |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2.21 ESSENTIAL PORTS/PROTOCOLS  (Indicate whether port tunneling is used) | | | | | | |
| Port | Protocol | Data Service | Source | Destination | Purpose |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.22 ESSENTIAL PROCESSESS | | | |
| Name | Object | Purpose |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.23 FILE SYSTEM  List all external interfaces that support file systems (USB, IEEE1394, SD, SIM) | | | |
| System | Purpose | Required? |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| 2.24 DOES THE SYSTEM EMPLOY TOKEN TECHNOLOGY?  (Non-rewritable access and PIN devices), if so describe its purpose. | |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.25 COMMERCIAL MANUFACTURER LEVEL OF FAMILIARITY  (With Department of Defense (DoD) Information Assurance Regulations/Forms/Concepts) | | | | |
|  | Highly Familiar | Somewhat Familiar | Unfamiliar |  |
| DoD 8500.1 Information Assurance |  |  |  |  |
| DoDI 8500.2 Information Assurance Implementation |  |  |  |  |
| DISA Security Technical Implementation Guide (STIG) |  |  |  |  |
| DISA Information Assurance Vulnerability Alert (IAVA) |  |  |  |  |
| DODI 8551.1 Ports, Protocols, and Services Management (PPSM) |  |  |  |  |
| DODD 8750.01 Information Assurance Workforce Improvement Program |  |  |  |  |
| DoD Notice of Consent Banner and User Agreement |  |  |  |  |
| DODI 8420.01 Commercial Wireless LAN Devices, Systems and Technologies |  |  |  |  |
| NIST FIPS 140-2 Security Requirements for Cryptographic Modules |  |  |  |  |
| Defense in Depth/Security Zones |  |  |  |  |
| Background Checks and Investigations |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.26 COMMERCIAL MANUFACTURER LEVEL OF FAMILIARITY  (With Department of Defense (DoD) Information Assurance Tools) | | | | |
|  | Highly Familiar | Somewhat Familiar | Unfamiliar |  |
| DISA Gold Disk |  |  |  |  |
| Security Technical Implementation Guide |  |  |  |  |
| Security Readiness Review (SRR) |  |  |  |  |
| Retina |  |  |  |  |
| NMAP |  |  |  |  |
| App Detective |  |  |  |  |
| NESSUS |  |  |  |  |
| NTO Spider |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.27 AUTHENTICATION  (Does your system support the following) | | | |
|  | Yes | No |  |
| DoD Password complexity rules (case sensitive, 14-characters, lower, upper, numeric, alphabetic, and special characters) |  |  |  |
| Password History/Aging (90 days) |  |  |  |
| Operating System services that utilize anonymous access |  |  |  |
| Biometrics |  |  |  |
| Public Key Infrastructure (PKI) using X.509 certificates |  |  |  |
| Remote Access authentication |  |  |  |
| Multi-factor |  |  |  |
| Certificates/Tokens |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.28 AUDITING  (Does your system support the following) | | | |
|  | Yes | No |  |
| Audit logs |  |  |  |
| Customizable audit levels |  |  |  |
| Retention settings for system logs |  |  |  |
| Audit logs protection from deletion |  |  |  |
| Are audit trail events date/time stamped? |  |  |  |
| 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? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.29 FIRMWARE (FW) | | | |
|  | Yes | No |  |
| Is the FW configuration password-protected? |  |  |  |
| Is there a FW master override provided by the vendor? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.30 ANTIVIRUS/ANTIMALWARE | | | |
|  | Yes | No |  |
| AV Position Paper (if available) |  |  |  |
| AV recommended best practices (if available) *\*List items which should be excluded from scanning.* |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.31 DATA AT REST (DAR) | | | |
|  | Yes | No |  |
| DAR Encryption Position Paper (if available) |  |  |  |
| DAR Encryption products and versions validated |  |  |  |
| DAR Encryption recommended best practices  *\*Provide technical recommendations that address the protection mechanisms of data at rest.* |  |  |  |
| DAR Physical Protection |  |  |  |
| DAR Removable Media *\*Does the system/device provide encryption of portable media.* |  |  |  |
| Backup Encryption supported algorithms (3DES/AES/RC4/Other) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.32 DATA IN TRANSIT (DIT) | | | |
|  | Yes | No |  |
| DIT Encryption Position Paper (if available) |  |  |  |
| DIT Encryption technologies and versions validated |  |  |  |
| DIT Encryption recommended best practices  \* Provide technical recommendations that address the protection mechanisms of data in transit. |  |  |  |
| DIT Physical Protection |  |  |  |
| DIT Bandwidth requirements |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.33 AVAILABILITY | | | |
|  | Yes | No |  |
| Availability Position Paper (if available) |  |  |  |
| Availability products and versions validated |  |  |  |
| Availability recommended best practices (if available) *\*Provide technical recommendations that address data availability.* |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.34 IPv6 | | | |
|  | Yes | No |  |
| IPv6 Position/Strategy Paper (if applicable) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.35 HOST-BASED INTRUSION DETECTION/PREVENTION SYSTEM (HIPS) | | | |
|  | Yes | No |  |
| Strategy Paper (if available) |  |  |  |

|  |  |
| --- | --- |
| 2.36 HOST BASED SECURITY SYSTEM (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 Systems (IPS) and host firewall. If the proposed system 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.* | |
|  |  |

|  |  |
| --- | --- |
| 2.37 INTRUSION DETECTION/PREVENTION SYSTEM (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.* | |
|  |  |

|  |  |
| --- | --- |
| 2.38 NETWORK LOGICAL ALLOCATION AND PLACEMENT  (Does not apply to standalone systems) | |
| *Network placement – Describe manufacturer recommendation for system placement and considerations should the proposed system require physical and/or logical relocation. Describe network addressing requirements, segmentation, latency and/or performance issues that might arise as a result of system relocation.* | |
|  |  |

|  |  |
| --- | --- |
| 2.39 SYSTEM RECOVERY/LOSS  (Applies to laptops, tablets, and portables only.) | |
| *Accidental loss – Describe whether the proposed portable system supports remote wipe and/or geo tracking services in the event of accidental loss, theft, misplacement.* | |
|  |  |

|  |  |  |
| --- | --- | --- |
| 2.40 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 GOVERNMENT/INDUSTRY MANUFACTURING CERTIFICATIONS  (For example NIST FIPS, UL, FCC, TAA, TPM) | | |
| *Certifications - List all Government and Industry certifications associated with the system. Please provide proof of certification. For example, FIPS-140-2, FDA 510K.* | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.42 SYSTEM USER DESCRIPTIONS  (For example iHE, DICOM) | | |
| Role | Minimum Access Level |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.43 SECURITY ASSESSMENTS | | |
| Security Assessment Position Paper (if available) |  |  |
| Validated Security Assessment Tools |  |  |
| Recommended practices (if available) |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.44 WIRELESS | | | |
| State whether the 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? |  |  |  |
| Wireless Mode of Operation ad hoc? |  |  |  |
| Wireless Mode of Operation infrastructure? |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.45 WIRELESS – IEEE 802.15 BLUETOOTH  (Wireless Personal Area Network – WPAN) | | | | |
| Frequency (GHz) | Modulation | Throughput (Mbps) | Range (ft) (indoor/outdoor) |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.46 WIRELESS – IEEE 802.15 Zigbee | | | | |
| Frequency (GHz) | Modulation | Throughput (Mbps) | Range (ft) (indoor/outdoor) |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.47 WIRELESS – IEEE 802.15 (a/b/g/n) | | | | |
| Frequency (GHz) | Modulation (FHSS/OFDM/DSSS/CCK) | Throughput (Mbps) | Range (ft) (indoor/outdoor) |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.48 WIRELESS – OTHER – ULTRA WIDE BAND (UWB), IEEE 802.16  WiMAX, IR/MICROWAVE, ULTRASOUND, RADIO | | | | |
| Frequency (GHz) | Modulation | Throughput (Mbps) | Range (ft) (indoor/outdoor) |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.49 OTHER | | |
| Power Requirements (Voltage/Amps): |  |  |
| Weight (lbs.) |  |  |
| Physical Dimensions (H/W/D): |  |  |
| Environmental specifications: |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.50 PHYSICAL SAFEGUARDS | | | |
|  | Yes | No |  |
| 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? |  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.51 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – PRODUCT MANAGER (PM) | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.52 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – APPLICATION ENGINEER | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.53 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – NETWORK ENGINEER | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.54 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – SECURITY MANAGER | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.55 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – VULNERABILITY REMEDIATION | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 2.56 COMMERCIAL POINT OF CONTACT (POC) INFORMATION – INCIDENT REPORTING | | |
| Name | Phone | E-Mail |
|  |  |  |
|  |  |  |

Submitted By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_