DEFENSE HEALTH AGENCY (DHA)
MEDLOG CYBER Logistics CyberLOG
693 Neiman Street
Ft. Detrick, Maryland 21702

Medical Device and Equipment (MDE) Risk Assessment Questionnaire

MDERA

Version 4

To ascertain security compliance that is in agreement with United States Federal Government (USFG), Department of Defense (DoD), and Defense Health Agency (DHA) policies and directives, DHA Cyber Logistics (CyberLOG) requires the vendor complete the following Medical Device and Equipment (MDE) Risk Assessment (MDERA) questionnaire.

All MDE is subject to compliance with DoD and National Institute of Standards and Technology (NIST) cybersecurity requirements. The information recorded in this questionnaire, shall be used throughout the pre-acquisition/selection process in which the MDERA serves as the foundational point of data collection for cybersecurity evaluation and decision actions leading to an MDE Risk Management Framework (RMF) Authorization/Approval.

Failure to disclose all required information, or misrepresentation of the proposed MDE's capabilities, configuration, or intended mode of operation, shall result in the system being ineligible for acquisition, or result in a breach of contract and subsequent cancellation of the same if discovered after award.

The information provided below which includes configuration, current security posture, and level of compliance with the cybersecurity principles of Confidentiality, Integrity, and Availability, shall be used to identify the technical characteristics of the MDE and aid in the determination of the recommended RMF Level of Effort (LOE) and potential actions required prior to and during the Authorization/Approval process.

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

Revision History

Date	Section/Item	Comments	Author
Jan-13-2021	Full document	Redaction of the entire MDERA questionnaire	Walter J. Sandman (CIV)

UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN COMPLETED

READ BEFORE PROCEEDING:

The commercial vendor shall complete the Medical Device and Equipment Risk Assessment (MDERA) questionnaire in its entirety as part of the Request for Information (RFI) process.

Completion of this questionnaire is required for networked and/or standalone MDE.

References to external documents, publications or product literature are not acceptable.

Once completed, you may submit the MDERA questionnaire to the DHA CyberLOG Policy and Support Branch at the following e-mail address:

dha.detrick.med-log.list.cyberlog-plcy-spt@mail.mil

The CyberLOG Policy and Support Branch will contact the requestor within 72 hours of receipt of the questionnaire.

PRIMARY VENDOR POINT OF CONTACT (POC) INFORMATION (Vendor Account Manager)		
Name:		
Job Title:		
Company:		
Business Address:		
E-Mail Address:		
Phone Number:		
Web page Address:		
Signature and Date: (Signature indicates acceptance that all provided information is accurate, and that no information has been omitted) If Digital Signature is not possible, print and sign this page only. Attach scanned copy to the document.		DATE:

VENDOR TECHNICAL POINT OF CONTACT (POC) INFORMATION (Cybersecurity/Technical Representative)		
Name:		
Job Title:		
E-Mail Address:		
Phone Number:		
Signature and Date: (Signature indicates acceptance that all provided information is accurate, and that no information has been omitted) If Digital Signature is not possible, print and sign this page only. Attach scanned copy to the document.		DATE:

Section 1 – Identification and Regulatory Information		
1.0 MDE Title/Version: Provide the naming convention for the MDE		
1.1 MDE Category: Indicate the category/type of the MDE based on its intended use. You may also include the ECRI nomenclature identifier, if known		
1.2 MDE Description: Provide a description of the MDE. If applicable, you may include information found in the Summary page of the FDA 510K Premarket Authorization for regulated Medical Devices		
1.3 MDE Alternate Name: Indicate whether the MDE is marketed by any other name, model, trademark, or product family		
1.4 Regulated MDE: If applicable, provide the Food and Drug Administration (FDA) 510K Premarket Authorization identifier		
1.5 MDE Product Lifecycle: Indicate which predicate device this MDE is intended to replace		
1.6 MDE Production and Support Lifecycle: Specify the MDE product lifecycle dates	Initial Release Date:	End of Life Date:
1.7 Risk Management Framework (RMF): State whether the MDE has been or is currently undergoing the RMF Authorization/Approval process. If known, provide the name of the RMF Authorization repository and its unique record identifier. For Cloud-based systems, provide the Fed RAMP record identifier		
1.8 Baseline testing location: Indicate whether a pre-production instance of the MDE is available at the vendor's facility to serve as a test baseline location for product evaluation and vulnerability scanning. If so, provide location		

Section 2 – Operation and Deployment	
2.0 Intended Mode of Operation: Select the intended mode of operation of the MDE in accordance with manufacturer's recommended configuration.	☐ Standalone – MDE operates in complete physical and logical isolation. Data communication interfaces and associated networking protocols, including legacy serial RS-232 are not used. ☐ Peer to Peer LAN – Operates in logical isolation but requires the use of networking protocols or RS-232 serial data communications for host-to-host connectivity. ☐ Client/Server – Operates as a distributed application that partitions task or workloads between the service requester (client) and the service provider (server) using networking protocols. ☐ Web based - Client side application – Operates as a distributed application that requires the use of a client side browser and locally installed applets to access the Primary Application. Applets must be digitally signed by the server. ☐ Web based - Zero Footprint client side application. Operates as a distributed application that does NOT require the downloading and installation of server side software to access the Primary Application. This may also be referred to as Server-side rendered application. ☐ Host-based Device – Operates as a passive subsystem, which requires a dedicated connection to a host computer to produce information. It requires the use of networking protocols and/or legacy RS-232 serial data communications. ☐ Cloud-based – Operates within a cloud-service environment ☐ Government Cloud Service Provider ☐ Commercial Cloud Service Provider
2.1 Intended Method of Implementation: Select the intended method of implementation of the MDE.	☐ System comprises Hardware + Software + Firmware (traditional configuration) ☐ System is Software Only in a Physical Environment (requires hardware provided by the Department of Defense/Defense Health Agency ☐ System is Software Only in a Virtual Environment (requires virtual environment) ☐ Virtual Environment is provided by the Department of Defense/Defense Health Agency ☐ Department of Defense/Defense Health Agency must provide all Operating System/Database/Application Virtual Servers. ☐ Virtual Operating System (VOS)/Hypervisor provided by the Vendor

Section 2 – Operation and Deployment	
2.2 Interfaces Describe how the device connects to the Local Area Network (LAN), or the intended mode for communications.	☐ Serial RS-232 ☐ RJ-45 Networked ☐ Serial to RJ-45 Connection ☐ 802.11 Wireless ☐ Other (Specify Connection Type Below)
2.3 Externally Connected Systems Describe the types of systems that this MDE is required to interface with in order to operate as intended.	
2.4 DNS Realm/Active Directory Integration Indicate whether the MDE can support full/partial integration into a Microsoft Active Directory (AD) Domain.	
2.5 Endpoint Protection Indicate whether the MDE can/cannot support, either fully or partially, software based endpoint protection technology. Endpoint technology encompasses Antimalware, Host-based IPS/IDS, Asset Publishing, Data Loss Protection (DLP), and Application Whitelisting.	
2.6 Vulnerability Scanning When not in use, indicate whether the MDE can/cannot undergo automated credentialed vulnerability scanning. If not, please describe in detail the technical/operational limitations that prevent credentialed vulnerability assessment. Note: DHA CyberLOG reserves the right to perform non-invasive non-credentialed (passive) Discovery scans when the MDE is not use.	

Section 2 – Operation and Deployment	
2.7 Security Patching and updating Indicate whether the MDE can support either manual or automated security patching or updating. 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.	
2.8 Authentication Credentials Describe the type and purpose of all user accounts required by the MDE.	
2.9 Mass Storage Indicate whether the MDE requires the use of removable media and whether this information can be protected from unauthorized disclosure using Data at Rest (DAR) Full disk encryption.	

Section 3 – Configuration and Architecture

3.0 - Hardware

Component	Virtual /Physical	Manufacturer	Model	Serial Number	Operating System	End of Support

3.1 – Software

Application	Version	Manufacturer	Purpose

NOTE: You may attach additional configuration information on a separate document.

Section 3 – Configuration and Architecture				
3.2 - Data Communications				
Data Service	Protocol	Low Port	High Port	Purpose

UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN COMPLETED

Section 3 – Configuration and Architecture

3.3 - Architecture Diagram

Section 4 – Privacy	
4.0 Personally Identifiable Information: Identify from the list below, all the PII data elements processed by the MDE. • Biometrics • Citizenship • Driver's License • Employment Information • Home/Cell Phone • Mailing/Home Address • Military Records • Official Duty Address • Passport Information • Place of Birth • Race/Ethnicity • Records • Work E-Mail Address • Birth Date • Disability Information • Education Information • Financial Information • Law Enforcement Information • Marital Status • Mother's Middle/Maiden Name • Official Duty Telephone • Personal E-Mail Address • Position/Grade • Rank/Title • Security Information • Child Information • DoD Identification Number • Emergency Contact • Gender/Gender Identification • Legal Status • Medical Information • Name (s) • Other ID Number • Photo • Protected Health Information • Religious Preference • Social Security Number • Other	

END OF THE QUESTIONNAIRE – DO NOT WRITE BEYOND THIS LINE

REVIEW AND QUALIFICATION	
MDERA submitted to Vendor on:	
Agreed upon Estimated Time of Completion:	
Completed MDERA received on:	
MDERA QC Determination:	
Determination Rationale:	
LOE Recommendation:	
LOE Rationale:	
CAB Recommendation:	
CAB Rationale:	
Title/Acronym Naming Recommendation:	
EDMS container created on:	
PIA completed on:	
Observations:	
Total number of assets reported by JMAR:	
Total number of assets reported by Vendor:	
EHR integration approval status:	
MDE Final Disposition/ALT:	
MDE Recommended Priority:	
MDERA Reviewed By:	