Defense Health Agency

PROCEDURAL INSTRUCTION

NUMBER 8400.01
March 2, 2020

AD-CS/MEDLOG

SUBJECT: Cybersecurity Logistics (CyberLOG) Medical Devices and Equipment (MDE) Risk Management Framework (RMF)

References: See Enclosure 1.

1. PURPOSE. This Defense Health Agency-Procedural Instruction (DHA-PI), based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (t) establishes centralized processes and procedures to implement and maintain RMF authorization and cybersecurity for MDE across the Military Health System (MHS) through the Defense Health Agency (DHA) CyberLOG.

2. APPLICABILITY. This DHA-PI applies to all personnel to include: assigned or attached active duty and reserve Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA, to include DHA components such as regional and field activities (remote locations), and subordinate organizations administered and managed by DHA, to include military medical treatment facilities (MTFs) under the authority, direction, and control of the DHA.

3. POLICY IMPLEMENTATION. It is DHA's instruction, pursuant to References (d) through (t), that this CyberLOG:

a. Develop the standard DHA cybersecurity requirements process to translate and identify MTFs MDE planning requirements.

b. Implement a standard cybersecurity approach to analyze, evaluate, and manage MDE planning, procurement, and sustainment to meet cybersecurity requirements through the RMF process.

c. Execute the DHA RMF authorization process within DHA activities for MDE purchased with DHP funds.

d. Maintain an acceptable security baseline for MDE as defined in References (p) and (q).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This DHA-PI is available on the Internet from the Health.mil site at: www.health.mil/DHAPublications.

7. EFFECTIVE DATE. This DHA-PI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with Reference (c).

RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 2018
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018
(d) Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016
(e) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 as amended
(f) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(g) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended
(h) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended
(i) DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014, as amended
(j) National Institute of Standards and Technology Special Publication 800-30 Revision 1, "Guide for Conduction Risk Assessments," September 2012, as amended
(k) National Institute of Standard and Technology Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," February 2010, as amended
(l) National Institute of Standard and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015 as amended
(m) National Institute of Standard and Technology Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," September 2011
(n) DoD 8570.01-M, "Information Assurance Training, Certification, and Workforce Management," December 19, 2005, as amended
(o) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended
(p) DHA-Interim Procedures Memorandum 18-013, "Risk Management Framework (RMF)," October 10, 2018
(q) DHA-Interim Procedures Memorandum 18-015, "Cybersecurity Program Management," October 17, 2018
(r) Committee on National Security Systems Instruction 4009 IA "Committee on National Security Systems (CNSS) Glossary," April 6, 2015
(s) DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019
(t) OMB Circular A-130, "Managing Information as a Strategic Resource."

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will:

a. Assign responsibility for tracking compliance with the standard processes, procedures, and appointment types outlined in this DHA-PI to the Assistant Director, DHA Combat Support.

b. Implement policy, guidance, and instruction consistent with References (a) through (t).

2. ASSISTANT DIRECTOR, COMBAT SUPPORT. Assistant Director, Combat Support, will:

a. Exercise overall responsibility for the DHA CyberLOG.

b. Oversee the execution and accountability monitoring of standard processes, procedures, and appointment types by DHA CyberLOG.

c. Support strategies and programs through the responsibilities outlined in References (a) through (t).

3. DEPUTY ASSISTANT DIRECTOR (DAD) MEDICAL LOGISTICS (MEDLOG). The DAD-MEDLOG will:

a. Ensure MTFs establish MDE cybersecurity procedures in the MDE requirements process.

b. Provide strategic oversight for MDE cybersecurity implementation for DHA components in accordance with References (p) and (q).

c. Recommend and track measures to cybersecurity workload, performance, and compliance with the business rules and processes outlined in this DHA-PI.

d. Support strategies and programs through the responsibilities outlined in References (a) through (t).

4. CHIEF, MARKET TECHNOLOGY INTEGRATION OFFICE (MTIO). The Chief, MTIO, will:

a. Ensure support and communication to all MTF Information System Security Managers (ISSM) and Directors regarding compliance and implementation of MDE RMF within designated geographic markets.

b. Serve as the primary coordination point for implementation, sustainment and decommissioning efforts related to CyberLOG RMF activities.

c. As part of the single point-of-accountability function for DAD-IO, ensure satisfactory delivery of CyberLOG capabilities and the procedures within this DHA-PI.

d. Ensure pertinent MTIO personnel are assigned appropriate access in the CyberLOG Enterprise Document Management System (EDMS), Enterprise Mission Assurance Support Service (eMASS), business systems and the DHA HAR system for cyber vulnerability remediation.

5. CHIEF, DHA CYBERLOG DIVISION. The Chief, DHA CyberLOG Division, will:

a. Direct all DHA MDE cybersecurity activities and assist in coordination for MHS MDE. Orchestrate the planning, implementation, and prioritization of MDE cybersecurity workload and in coordination with functions across various organizations to include DHA Health Information Technology, Office of the Chief Health Informatics Officer, Services, etc.

b. Develop and maintain an organizational or system-level cybersecurity program that identifies architecture, requirements, objectives, policies, personnel, processes, and procedures to provide adequate security for all MDE assets in alignment with DHA Cybersecurity and RMF processes in accordance with Reference (q).

c. Serve as the RMF MDE integrator, ensuring cybersecurity requirements are incorporated for logistics, DHA Health Information Technology, operations, acquisitions, and clinical functions.

d. Advise the Enterprise on practical impacts and costs of cybersecurity policy.

e. Represent and communicate CyberLOG goals, values, and initiatives across the Enterprise.

f. Establish and report MDE cybersecurity metrics.

g. Ensure compliance with privacy regulations in accordance with References (s) and (t).

6. SUPPORT BRANCH CHIEF, DHA CYBERLOG. The Support Branch Chief, DHA CyberLOG, will:

a. Provide MDE cybersecurity liaison services and guidance for vendors, sites and organizations within the MHS.

b. Coordinate contacts and inquiries from external sources throughout CyberLOG.

c. Prioritize and streamline RMF MDE authorizations and processes to eliminate redundancy for the Enterprise.

d. Assist in the product selection process for MDE cybersecurity in accordance with Reference (q). Analyze the cybersecurity requirements and determine if the product meets cybersecurity requirements. Participate in DHA MEDLOG technical review and approval of MDE requirements.

e. Identify applicable MDE Security Technical Implementation Guides in partnership with the pertinent organizations.

f. Manage and track support requests for any items related to MDE cybersecurity activities or actions. See Enclosure 3 for communication plan.

7. OPERATIONS BRANCH CHIEF, DHA CYBERLOG. The Operations Branch Chief, DHA CyberLOG, will:

a. Maintain an accurate and detailed inventory of all MDE RMF authorizations.

b. Oversee entries of MDE into eMASS to ensure MDE mission requirements are met.

c. Coordinate with DAD-IO for independent verification and validation efforts, as well as Authorization to Operate (ATO) submissions for MDE under CyberLOG's area of responsibility.

d. Communicate with the DHA Cybersecurity Division (CSD) for new MDE standardization projects, strategic purchasing initiatives, and RMF-specific issues.

e. Support implementation of the RMF for MDE.

f. Maintain and report MDE assessment and authorization status and issues in accordance with cybersecurity requirements.

g. Coordinate with DHA CSD to ensure issues affecting the organization's overall security are addressed appropriately.

h. Act as the primary cybersecurity technical advisor in coordination with DHA CSD that may affect the MDE posture.

i. Review and endorse all Information System Security Authorization Packages prior to submitting to DHA CSD.

j. Maintain all RMF documentation and modifications pertaining to MDE in the CyberLOG container in eMASS.

k. Ensure that Cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.

8. SUSTAINMENT BRANCH CHIEF, DHA CYBERLOG. The Sustainment Branch Chief, DHA CyberLOG, will:

a. Implement and maintain continuous monitoring policies for MDE.

b. Perform continuous monitoring against MDE according to DHA CyberLOG MDE policies.

c. Maintain MDE security baseline and ensure it remains at an acceptable level commensurate with its authorization.

d. Manage MDE interconnectivity and remote access including government sponsorship for trusted commercial DoD partners utilizing the DHA Business to Business services.

e. Coordinate with external branches that oversee network configurations (i.e. Infrastructure and Operations / Engineering Solutions Architecture-Business Analytics Divisions, Group Policy) and (Cyber Operations Center for Host based Intrusion Protection System / antimalware) to analyze, address and resolve technical issues arising from improper network configurations including; access control lists, group policy objects, antimalware, and host based intrusion prevention system.

f. Upload vulnerability scans from MTFs data results produced by select MDE to DHA eMASS instance and ensure results are published to the continuous monitoring risk scoring system.

g. Assist MTF/Other Lines of Business (OLB) ISSMs with remediation actions of vulnerabilities in coordination with the CyberLOG Support Branch.

h. Ensure that cybersecurity-related events or configuration changes, that may impact MDE authorization or security posture, are formally reported to the CyberLOG Operations Branch, authorizing officials of other affected parties and interconnected DoD Information Systems.

i. Manage Plan of Action and Milestones (POAM) as applicable (mitigation strategies, completion dates, extensions, submission through the POAM package approval chain) once MDE receives authorization.

9. DIRECTOR, DHA MARKET. The Director, DHA Market, will ensure MTF compliance of procedures outlined in this DHA-PI.

10. MTF DIRECTORS AND OLB COMMANDING OFFICERS. MTF Directors and OLB Commanding Officers will:

a. Adhere to responsibilities listed Reference (e) and References (n) to (q), and all DHA cybersecurity policy and guidance for system/applications the MTF purchases.

b. Enforce DHA AO authorization decisions for hosted or interconnected Information Systems and Platform Information Technology systems.

c. Coordinate with the Market Director and/or MTIO to ensure compliance with this DHA-PI.

11. MTF CHIEF INFORMATION OFFICER (CIO) AND OLB CIOs. The MTF CIO and OLB CIOs will:

a. Adhere to CIO responsibilities listed in References (e), (n), (o), (p) and (q).

b. Provide CyberLOG the names of MTF appointed ISSMs/Information System Security Officers semi-annually via the CyberLOG organizational email address (dha.detrick.med-log.mbx.cyberlog@mail.mil).

c. Ensure MDE is installed consistent to the MDE authorization.

12. MTF AND OLB ISSMs. MTFs and OLBs ISSMs are the primary cybersecurity technical advisors to the MTF/OLB Director (program manager for the medical enclave), authorizing official, and information system owner. The MTFs and OLBs ISSMs will:

a. Adhere to ISSM responsibilities listed in References (e), (n) through (p), and (q).

b. Validate MTF MDE inventory data through available means, which can include discovery scans, eMASS record information, and data repositories (Joint Medical Asset Repository, Defense Medical Logistics Standard Support, and DoD Information Technology Portfolio Repository).

c. Obtain DHA eMASS access and request view only access to the CyberLOG container by submitting a Remedy request as described in Attachment 3.

d. Provide view only access to the CyberLOG group to the local eMASS enclave record in coordination with the CyberLOG support point of contact (POC).

e. Initiate fully credentialed vulnerability scanning as defined by the CyberLOG Sustainment Branch and MTF/OLB ISSM for continuous monitoring purposes.

f. Submit fully credentialed vulnerability scan report copies to the CyberLOG Sustainment Branch for continuous monitoring purposes via EDMS.

g. Submit make, model, and version to CyberLOG Support Branch after selection for new procurement of MDE by submitting a Remedy request as described in Enclosure 3 of this DHA-PI.

h. Validate the make, model, and version of current MDE inventory at their area of responsibility.

i. Submit a remedy ticket as described in Enclosure 3 of this DHA-PI in the absence of an existing ATO.

j. Initiate preliminary informational vulnerability scans as defined by the CyberLOG Support Branch and the MTF ISSM.

k. Be responsible for all applicable Defense Information Systems Agency Enterprise Network Security (also known as Host Based Security System). This requirement is applicable only to MDE certified as compatible by the MDE original equipment manager.

l. Assess applicable controls annually prior to the anniversary of the authorization date in accordance with the validation procedures in the RMF knowledge Services.

m. Complete quarterly reviews of MDE system controls to ensure annual review requirements are met.

ENCLOSURE 3

PROCEDURES

1. COMMUNICATION PLAN

a. MTF ISSMs can review the status of RMF efforts through eMASS CyberLOG container and Consolidated System Tracking and Reporting: (https://info.health.mil/apps/HIT/cstar/Pages/Dashboards.aspx).

b. CyberLOG will communicate MDE cybersecurity compliance issues with local MTF CIO after CyberLOG identification by submitting a remedy ticket as described in this DHA-PI.

c. MTF ISSMs will notify CyberLOG of any security incidents for MDE within one working day for CyberLOG assistance by submitting a remedy ticket as described in this DHA-PI.

d. MTF ISSMs will coordinate with CyberLOG prior to any configuration changes of MDE by submitting a remedy ticket as described in this DHA-PI.

2. MDE CYBERSECURITY HELP REQUEST

MDE CYBERSECURITY HELP REQUEST. MTF will contact the CyberLOG Support Branch for requests related to MDE Cybersecurity and RMF efforts. All help requests will be submitted via a remedy ticket (https://gsc.health.mil) or the CyberLOG Support Branch organizational formatted email box: (dha.detrick.med-log.mbx.cyberlog@mail.mil). Examples of typical help requests include, but are not limited to:

a. new MDE procurement requests for Cybersecurity review

b. ATO requests-for existing equipment (adding sites to eMASS record)

c. Business to Business interconnectivity request

d. Command Cyber Readiness inspection assistance

e. RMF assistance

f. security incident response support

g. ports, protocols, and services management update support

h. configuration management updates

i. authorization boundary support

j. POAM requests

k. Document verification requests

3. MDE CYBERSECURITY REQUIREMENTS OVERVIEW. The MDE Cybersecurity Requirements process is based on processes outlined in References (e) through (t).

a. All MDE requires a Cybersecurity assessment and approval.

b. For existing MDE, MTFs CIOs/ISSMs will submit the following items to the CyberLOG Support Branch in a remedy ticket: vendor, make, model, version, vendor POC, and site POC.

(1) Once the required information is submitted, the CyberLOG Support Branch will review the information and check for an existing assessment and approval. If an assessment and approval exist, CyberLOG will add the requesting MTF to the deployment location list within 10 working days.

(2) If no assessment and approval exist, the CyberLOG Support Branch will initiate and prioritize the RMF effort for the MDE request and will require fully credentialed vulnerability scans from the MTF or a manual assessment process approved by Chief, DHA CyberLOG Division.

c. MTFs will ensure the inclusion of the DHA CyberLOG cybersecurity language from the DHA CyberLOG SharePoint site in the purchase agreement/contract.

(1) Prior to award, MTFs will provide the DHA Medical Device and Equipment Risk Analysis filled out by the vendor and preliminary fully credentialed vulnerability scans covering all components of the device to the CyberLOG Support Branch. All MDE under consideration must be submitted to the CyberLOG Support Branch via EDMS for review and recommendation.

(2) Recommendations will be provided within 10 working days upon receipt of all artifacts for MDE under consideration.

4. CONTINUOUS MONITORING PROGRAM. POAM support for MDE:

a. MTFs contacts the CyberLOG Sustainment Branch for support related to MDE POAMs.

b. MTF will submit fully credentialed vulnerability scans via EDMS ensuring that there is no impact to healthcare delivery, in accordance with current policy.

(1) Prior to scan, ensure the MDE is not in use for patient care.

(2) Provide fully credentialed vulnerability scans to the CyberLOG Sustainment Branch for review.

c. MTF ISSMs maintains all MDE under their purview in accordance with the authorization baseline as recorded in eMASS. Report any deviations to the CyberLOG Sustainment Branch.

d. MTF ISSMs provide ad hoc scans upon request to the CyberLOG Sustainment Branch.

e. MTF ISSMs will notify the CyberLOG Sustainment Branch of MDE no longer used or in operation and provide MDE replacement information, if applicable.

f. MTF ISSMs will work with MDE Vendor to remediate vulnerabilities and comply with DoD cybersecurity requirements.

g. MDE not remediated from the MDE baseline will be reported to DHA Cyber Operations Center for action.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
CIO	Chief Information Officer
CSD	Cybersecurity Division
CyberLOG	Cybersecurity Logistics
DHA	Defense Health Agency
DHA-PI	Defense Health Agency-Procedural Instruction
EDMS	Electronic Document Management System
eMASS	Enterprise Mission Assurance Support Service
ISSM	Information System Security Manager
MDE	Medical Device and Equipment
MEDLOG	Medical Logistics
MHS	Military Health System
MTF	military medical treatment facility
MTIO	Market Technology Integration Office
OLB	Other Lines of Business
POAM	Plan of Action and Milestones
POC	point of contact
RMF	Risk Management Framework