DHA Cyber Logistics Center of Excellence

Defense Health Agency (DHA) Cyber Logistics (CyberLOG) Cybersecurity/Risk Management Framework (RMF) Requirements

Updated: March 25, 2019

Version Matrix

Version	Date	Author	Description
1.0	16 November 2018		Completed initial draft of Cybersecurity Language.
1.1	31 January 2019		Updated document to reflect vendor comments/suggestions.
1.2	06 February 2019	CyberLOG	Final Document
1.3	25 March , 2019	CyberLOG	Addition of Section B 1.11.

Table of Contents

Defense Health Agency (DHA) Cyber Logistics Cybersecurity/Risk Management Framework (RMF) Requirements

Version 3/25/2019

A. General Overview of DHA Cybersecurity Requirements

1. **New Equipment/Product systems, equipment and software under RMF**:
The vendor shall agree to comply with References listed in Appendix A.

1.1. Software patches and updates: Many enterprises within the DoD automate patch updates and software updates for operating systems and DoD standard software applications. For applications such as databases and developed applications, updates are scheduled. Vendors shall notify the assigned CyberLOG analyst of any updates/changes to the system prior to installation, to include but not limited to software updates, Operating System, or Application upgrades, patches, addition/removal of components. If the CyberLOG analyst is unknown, the vendor shall submit all requests to dha.detrick.med-log.mbx.cyberlog@mail.mil. Software updates will be analyzed by the Government to determine if reauthorization is required by Department of Defense Instruction (DoDI) 8510.01 Risk Framework (RMF) for DoD Information Technology (IT). Patches normally address bug fixes and cybersecurity issues. Applying patches usually does not trigger reauthorization. Per the DoDI 8500.01 Cybersecurity, Enclosure 3, paragraph 9.b. (11), "All CYBERSECURITY products and IA-enabled products that require use of the product's CYBERSECURITY capabilities will comply with the evaluation and validation requirements of Committee on National Security Systems Policy 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, June 2013, as amended."

1.2. Vendors shall comply with the National Information Assurance Partnership (NIAP) Common Criteria Cybersecurity Evaluation and Validation Scheme (CCEVS) evaluation (https://www.niap-ccevs.org) which is published on the NIAP-CCEVS Products Compliance List. The NIAP-certified products have been assessed from a security perspective, helping to reduce the existence of potential vulnerabilities. Vendors are required to continually maintain their products, mitigating vulnerabilities and distributing fixes to licensed users.

1.3. Reauthorization in accordance with DoD RMF requirements: Per DoDI 8510.01, Enclosure 6, para 2.f.(6).(a), "In accordance with Appendix III of Office of Management and Budget (OMB) Circular A-130, systems must be reassessed and reauthorized every 3 years or as a result of a system update that negatively affects the security posture (whichever is less)." Program Offices or appropriate logistics organizations plan for this activity. The results of an annual cybersecurity review or a negative change to the system or environment at any time (i.e., a change increasing the residual risk) may result in a need for reauthorization prior to the regular three-year reauthorization.

1.4. The vendor shall maintain all equipment/product versions provided pursuant to this contract, to include the supported operating system, by issuing patches/updates to mitigate vulnerabilities [e.g., Information Assurance Vulnerability Alerts (IAVA) or Information Assurance Vulnerability Bulletins

(IAVB)] and network security configurations [e.g., Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs)]. The vendor must adhere to DHA guidance for remediation or mitigation of vulnerabilities associated with the equipment/product. Vendors shall be responsible for providing CYBERSECURITY maintenance support for six (6) years, or until the end of life date of the equipment identified by the vendor, whichever is longer. The vendor shall include, in its pricing to the Government the cost of patching their equipment throughout its lifecycle.

2. **Pricing for Cybersecurity**:
If there are any additional costs associated with any element of the Cybersecurity lifecycle, the vendor shall include those costs as follows:

2.1. All costs to achieve the initial Authority to Operate (ATO) and maintain it during the equipment's warranty shall be included in the initial quote/offer price.

2.2. The cost of updating, and upgrading the vendor's equipment to maintain the ATO throughout its lifecycle, shall be covered in the vendor's post warranty maintenance offering. At a minimum, vendors must offer RMF only maintenance which shall cover only actions related to maintaining the ATO and providing continuous monitoring of the system. The Government would need to purchase the RMF maintenance on an annual basis, either individually or as part of their normal maintenance packages, in order to maintain the RMF coverage on a system. The vendor shall be required to provide RMF only maintenance option pricing or RMF coverage as part of higher level maintenance coverage, as required by the Request for Offer (RFO) or Request for Proposal (RFP), in their quote/offer, broken out by each year. This option pricing shall at a minimum be used in the evaluation/selection of vendors. The Government may choose to exercise the RMF only maintenance pricing or use the vendor's normal maintenance offering under their contract, if it includes Cybersecurity maintenance coverage. Vendors shall be required to have RMF only maintenance coverage on their multiple award basic contract or offer it on any single award contract in order to receive an order/contract, unless they agree to provide the patching, updates, upgrades, and monitoring at no charge to the Government for six (6) years or as long as the system is commercially available, whichever is longer. Furthermore, the vendor agrees they will offer RMF only maintenance coverage on their contract for six (6) years or as long as the system is commercially available, whichever is longer.

3. **Maintenance and upgrades:**
Vendors shall agree to the DHA Cybersecurity requirements as outlined in this document for all systems and medical devices, unless an exception has been granted for a system by the Government prior to award/order issuance.

B. DHA Cybersecurity/Risk Management Framework (RMF) Requirements

1. **System Security Requirements**

1.1. The vendor shall submit to the Government, included in the offer/quote, all sections of the Medical Device Equipment Risk Assessment (MDERA Questionnaire), which is provided by the government. Additionally, a vulnerability assessment/report is required from a NESSUS scanner as this is the DoD standard. Vendors must provide a fully-credentialed NESSUS scan with RFO submission, and monthly Nessus scans provided by the tenth (10^{th}) day of the month after award.

1.2. Vendor agrees to comply with security regulations and guidance listed in Appendix A: Cybersecurity Regulations and Guidance and all RMF requirements.

1.3. Failure to meet the requirements may result in termination of the delivery order for cause, in accordance with Federal Acquisition Regulation (FAR) 52.212-4(m).

1.4. The vendor device or system shall pass pre-validation technical screening (vulnerability scans utilizing NESSUS, Security Content Automation Protocol (SCAP) scans, and Security Technical Implementation Guides (STIGs) checklists) within 6 months of contract award. All technical scans will be provided by the vendor to the Government PM for review. Vendor Medical Device and Equipment (MDE) shall pass fully credentialed screening given DHA approved template. Successful pre-validation technical screening must meet the Cybersecurity criteria listed below:

1.4.1. No unmitigated Very High or High Severity/ Category I (CAT I), vulnerabilities as described in the appropriate Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) located on http://iase.disa.mil/stigs/Pages/index.aspx

1.4.2. No unmitigated Moderate Severity/Category II (CAT II), vulnerabilities described in the appropriate Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) located on http://iase.disa.mil/stigs/Pages/index.aspx

1.4.3. No unmitigated Very High or High Severity/ Category I (CAT I) vulnerabilities from Nessus vulnerability scans.

1.4.4. No unmitigated Moderate Severity/ Category II (CAT II) vulnerabilities from Nessus vulnerability scans.

1.5. The government will provide templates of all requested technical documentation no later than twenty (20) days from date of initial contact from the vendor. Initial response and acknowledgement from the vendor is due within ten (10) working days of delivery of the templates. The Vendor shall remit all requested technical documents to the requestor no later than one hundred and thirty (130) days from the Date of Order.

1.6. The vendor shall mitigate all Very High, High, and Moderate Severity/CAT I, and CAT II vulnerabilities discovered during the RMF Assessment process according to the associated Plan of Action & Milestone (POA&M).

1.7. The vendor shall provide a Point of Contact (POC) responsible for the cybersecurity of the vendor device or system, throughout the lifecycle of the system. The vendor shall provide Subject Matter Experts (SMEs) to support all assessments of contracted products and materials outlined in the chart in paragraph 2.

1.8. For all equipment requiring a full Independent Verification and Validation (IV&V) test, the vendor shall not make any delivery and shall not receive payment for the system until the Program Management Office (PMO) has completed a self-assessment, and the IV&V has been scheduled. IV&V cannot be scheduled until all documentation requirements, and technical requirements have been completed to the PMO's satisfaction. Additionally, all identified POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and Protected Health Information (PHI)/Personally Identifiable Information (PII)/For Official Use Only (FOUO) data housed within the system. Delivery may take place prior to this milestone (IV&V scheduling) only if written permission is provided by the Contracting Officer.

1.9. For all equipment requiring an Assess Only certification, the vendor shall not make any delivery and shall not receive payment for the system until the PMO has completed a self-assessment, and the system has been submitted for an Assess Only ATO/APL. Submission cannot be scheduled until all documentation requirements, and technical requirements have been completed to the PMO's satisfaction. Additionally, all identified POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and PHI/PII/FOUO data housed within the system. The vendor must receive written confirmation from the PMO or Contracting Officer that the system has been submitted for an assess only ATO/APL and that the vendor may proceed with delivery. Delivery may take place prior to this milestone only if written permission is provided by the Contracting Officer.

1.10. The vendor shall obtain a recommendation of ATO from a Government-appointed third party validator within twelve (12) months of contract award for technologies processed through an Assessment & Authorization (A&A). Additionally, the vendor shall obtain an authorization from a Government official to be added to an APL for systems/devices processed through an RMF Assess Only.

1.11. Prior to final acceptance and installation, the vendor shall ensure that the delivered device matches the DoD authorized configuration. The vendor shall coordinate running Nessus and SCAP scans with the site and the assigned

CyberLOG Analyst to verify compliance. Any deviations will require the vendor to bring the system into compliance before final acceptance.

1.12. Pursuant to subsequent warranty period and Service Maintenance Agreements (SMAs), the vendor shall, after the issuance of an ATO or APL approval, ensure that the vendor's device or system maintains its ATO or operating system platform and patches/updates for six (6) years or as long as the vendor commercially supports the equipment/product, whichever is longer.

The vendor shall maintain an ATO or APL approval on all equipment/product versions owned by the Defense Health Agency (DHA) and Services and originally purchased through the vendor's contract. If a vendor cannot support the ATO or APL approval for all DHA/Service owned versions of the equipment/product, the vendor can meet this requirement by offering to provide all upgrades to the equipment/product that are required to maintain the ATO or APL approval, either at no cost to the Government or at a fixed price that is included in a RMF only maintenance offering under the vendors contract. During the period of time the vendor has a product installed on the network, the vendor shall provide all required cybersecurity patches/updates. Maintaining the RMF ATO or APL approval shall be included as part of the vendor's warranty period. For updates/patches, executable files should be distributed by the manufacturer accordingly, or implemented by the manufacturer's technical staff, dependent on the Service Agreement processes.

1.13. The vendor shall establish appropriate administrative and technical safeguards to ensure the confidentiality, integrity, and availability of Government data under their control.

1.14. The vendor shall notify the PMO and Contracting Officer POCs in writing with any inabilities to comply with DoD security requirements. Vendor will provide anticipated costs and timelines required to address any vulnerabilities in question.

1.15. The vendor shall contact the IA/RMF Office Representative, no later than five (5) business days after delivery order issuance or contract award, to start the process. Failure to do so would be considered a vendor-caused delay.

1.16. The proposed system shall be Internet Protocol version 6 (IPv6) capable or the vendor shall provide a detailed project, migration or planning documentation to show when the proposed system shall be IPv6 capable.
Minimum IPv6 capabilities include:

- Conformant with the IPv6 standards profile contained in the DoD IT Standards Registry (DISR);
- Maintaining interoperability in heterogeneous environments with IPv4;
- Commitment to upgrade as the IPv6 standard evolves;
- Availability of vendor IPv6 technical support.

1.17. The contractor shall be able to demonstrate or provide documentation to prove that their product is IPv6 capable.

2. **RMF Assessment Timeframes**

2.1. **Required Vendor Timeframes**: The Government shall complete its required actions within the following referenced timeframes but no later than one year after order/contract issuance. If the vendor has completed all required actions in a timely manner and acceptable manner while the Government experiences delays, the vendor would be given additional time for future actions corresponding to the amount of Government delay.

Vendor Requirements:	**Initial Draft Date Due**	**Final Date Due**
Vendor to contact Gov POC **dha.detrick.med-log.mbx.cyberlog@mail.mil**	10 business days post award	-
Hardware/Software/Architecture Documents	15 business days post award	20 business days post award
RMF Documentation Production	6 weeks post award	4 months post award
Technical Nessus Scans	1 month post award	6 months post award
Technical STIG Checklists	1 month post award	6 months post award
Technical SCAP	1 month post award	6 months post award

2.2. **Required Vendor Timeframes**: The Government shall complete its required actions within the following referenced timeframes but no later than one year after order/contract issuance. If the vendor has completed all required actions in a timely manner and acceptable manner while the Government experiences delays, the vendor would be given additional time for future actions corresponding to the amount of Government delay.

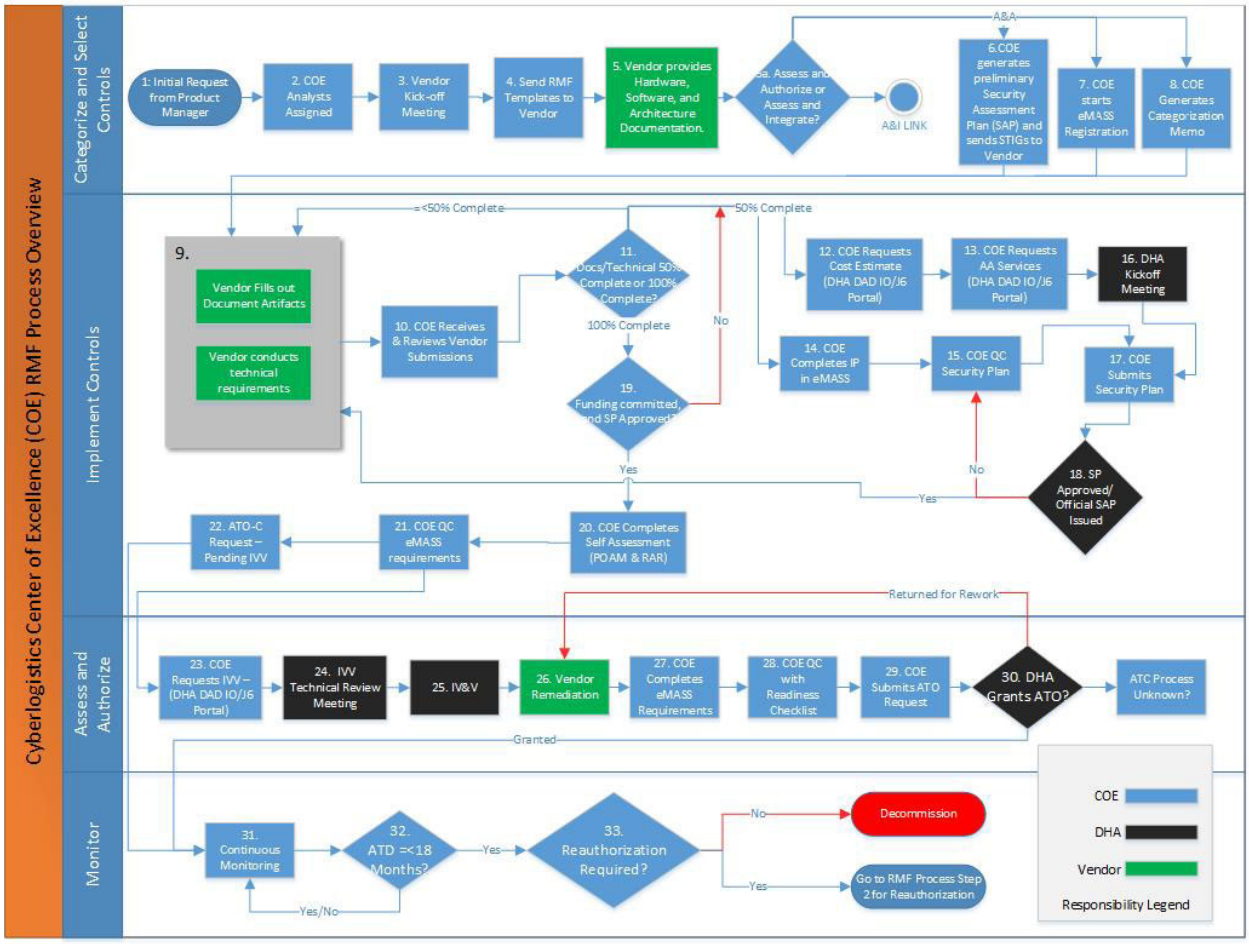
Government Requirements	**Initial Draft Date Due**	**Final Date Due**
Kickoff Meeting	15 business days post award	-
Security Assessment Plan Generation	20 business days post award	30 days post award
RMF Templates sent to Vendor	5 business days post vendor initial contact	-
Copies of Applicable STIGs sent to Vendor	17 business days post award	30 days post award
Authorization to Operate with Conditions (ATO-C) Recommendation	ATO-C recommendation submitted to 3rd party validator 2 weeks after final	

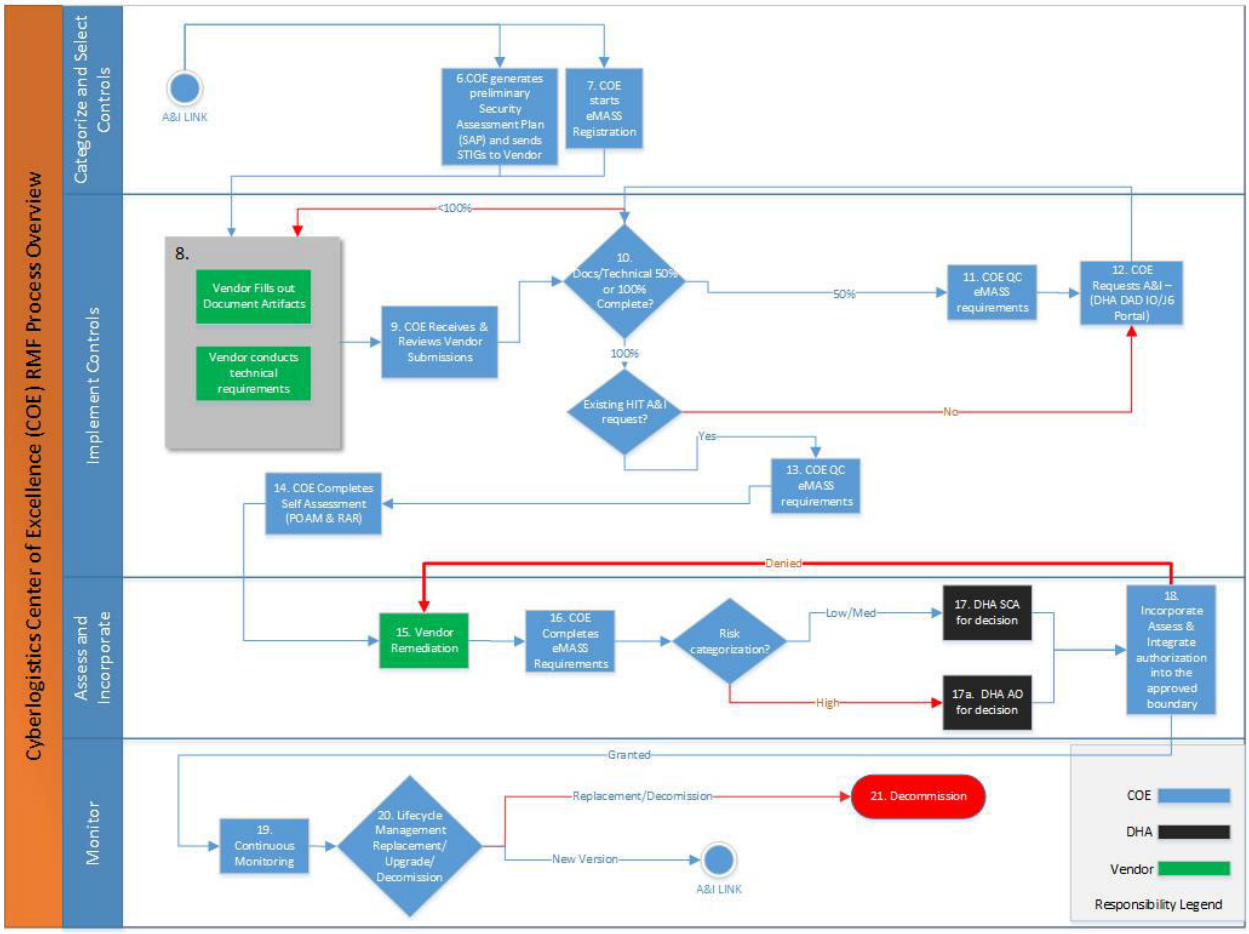
	documentation/technical scans received	
Independent Verification and Validation (IV&V) Scheduling	Scheduling request to 3rd party validator 3 weeks after final documentation/technical scans received	

2.3. **Informational Overview of the RMF Process**: The following diagrams provide a summary overview of the entire process to obtain approval under DHA Cybersecurity requirements. These diagrams are for informational purposes only, are not contractually binding, and subject to change without notice. Above tables contain the contractual requirements that must be met.

DHA Cyber Logistics Cybersecurity/Risk Management Framework (RMF) Requirements

Version 3/25/2019





Note: Not all above actions occur in a sequential manner, as some actions may be worked concurrently.

3. Assessment and Authorization (A&A)

3.1. The vendor shall provide hardware/software lists, architecture drawings, and workflow drawings within fifteen (15) business days after contract award. The vendor shall submit all other RMF-required documentation for review and approval, no later than four (4) months after receipt of the templates provided by the Government.

3.2. The vendor shall obtain approval from the Government for any vendor-developed RMF policies, plans, and procedures, prior to implementation.

3.3. The vendor shall provide any additional documentation required by the Government for completion of the A&A process within thirty (30) business days of a request by the Government.

3.4. The vendor shall provide technical scans within one (1) month of the A&A kickoff meeting.

3.5. The vendor shall provide updated technical scans on a monthly basis, on the 10th day of each month until an ATO is granted or the product is added to the APL.

3.6. In accordance with DoD 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems, incorporating Change 1, October 27, 2017 Section 2.0 INFORMATION SAFEGUARDS, the vendor shall ensure that the selected MDE is capable of supporting the use of DISA approved intrusion detection and prevention, antivirus, and anti-malware applications that are approved at the time of the ATO or APL issuance. The vendor device or system must be configured in such a way that allows the updating of malware definition signatures on a scheduled basis. Scanning shall encompass the entire system (file system, operating system, and real-time processes) by default. In cases where scanning of the entire system may negatively affect its operation, the vendor shall provide a detailed list of exclusions with justifications. The vendor shall provide technical specifications that clearly demonstrate whether the proposed solution can integrate and support either the full security suite or the individual components (e.g. Data Loss Prevention (DLP), Intrusion Prevention System (IPS), Antivirus, etc.) without performance degradation of the vendor device or system. In cases where the operation of security applications are not technically achievable, the vendor shall provide detailed justification and a POA&M describing steps towards compliance with this requirement.

4. Privileged User Training and Certification Requirements

4.1. If a vendor requires a Business-To-Business (B2B), access, etc. to government networks to maintain, analyze, etc., their equipment/product, they must adhere to the following requirements:

4.2. Information Assurance Contractor Training and Certification. Contractors requiring a privileged-level account for administrative/maintenance support of systems/applications on the DHA network will meet DHA requirements for a privileged-level account before being granted a network account. Requirements include:

4.2.1. Cyber (Information assurance (IA)/information technology (IT)) certification. Per DoD 8570.01-M and DFARS 252.239.7001, the contractor employees supporting Cyber (IA/IT) functions shall be appropriately certified upon contract award. Contractors will be defined at Information Assurance Technical level I (IAT Level I) and be required to meet minimum Professional Baseline certifications at the time of the contract award. Contractors will be given six (6) months to meet Computer Environment (CE) and Cyber Security Fundamental training

requirements. Not meeting the requirements in accordance with DoD 8570.01-M will result in the contractor account and access being 'Disabled' or 'Deleted' until such time as the conditions of this contract are met.

4.2.2. Background Investigation. National Agency Check with Local Agency Check and Credit Checks (NACLC) or above is required.

4.2.3. Professional Baseline Certification. The minimum Professional Baseline certification for IAT-II are: CCNA Security, CompTIA Cyber Security+. Higher certifications (GSCL, CISM, CISSP, etc.) will satisfy this requirement.

4.2.4. Computer Environment (CE) Certification. The CE certifications are determined by the role of the contractor and must be met within six (6) months of delivery order issuance in accordance with DoD 8570.01-M.

4.2.5. Two-Factor Authentication. Contractors will authenticate using two-factor authentication. The only method for authenticating is the Common Access Card (CAC).

4.2.6. Network Account Request Package (Authorized & Privileged). The contractor will submit a request package through either the facility Provost Marshall Office in conjunction with the facility Information Management Department (for contractors requiring on-site access), or through the Information Assurance/Cyber Security Branch (for contractors requiring remote access to a DHA network). Remote access must be through a DISA B2B solution.

4.2.7. The CYBERSECURITY Training. DoD Cyber Awareness Challenge Training must be completed by all contractor employees and associated sub-contractor employees prior to issuance of network access and annually thereafter. DoD Cyber Awareness Challenge Training is available at the following website: https://iase.disa.mil/eta/Pages/online-catalog.aspx

4.2.8. Personally Identifiable Information Training (PII). DoD PII Training must be completed by all contractor employees and associated sub-contractor employees prior to issuance of network access and annually thereafter. DoD PII Training is available at the following website: https://iase.disa.mil/eta/Pages/index.aspx

4.2.9. Health Insurance Portability and Accountability Act (HIPAA) Training. DoD HIPAA Training must be completed by all contractor employees and associated sub-contractor employees prior to issuance of network access and annually thereafter. DoD HIPAA Training is available at the

following website: https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf?ORG=MHS

4.2.10. Acceptable Use Policy (AUP). All vendors/contractors will sign/acknowledge the DHA Standard Acceptable Use Policy (AUP) prior to being granted a DHA network account. The DHA Standard AUP is available at the following website: https://health.mil/Reference-Center/Policies?query=Acceptable%20Use

5. **Warranty and Post-Warranty Service Maintenance Agreement Cybersecurity Requirements/Continuous Monitoring/Risk Management.**

5.1. Using a test/laboratory environment, the vendor shall be able to duplicate all fielded equipment/product that falls under the authorization boundary. The vendor shall ensure that all fielded equipment/product falling under one authorization is tested to maintain the ATO or approved products for as long as the vendor commercially supports the equipment/product. For each version owned by DHA and originally purchased through the vendor's contract, the vendor will ensure that each component within the authorization boundary is represented in the test group.

5.2. The vendor shall update all ATO or approved products required supporting documentation in the event of a system policy, procedural, logical or technical changes to the system or device.

5.3. The vendor shall maintain the authorized security configuration and notify the government within forty eight (48) hours of any changes for review. A major upgrade such as major software or hardware revision must be reassessed for ATO or addition to the approved products list. Minor upgrades must be assessed by the Government to determine if a reauthorization is required. The Vendor shall support reauthorizations due to both major and minor upgrades.

5.4. The vendor shall ensure the vendor's device or system is in compliance with the Department of Defense (DoD) Information Assurance Vulnerability Management (IAVM) program upon each deployment.

5.5. The vendor shall ensure any new deployment (including rebuilds) deploys with a fully-patched, accredited version.

5.6. The vendor shall maintain the system or device and update to comply with updated STIGs made available by the Government within three (3) months of notification by the Government.

5.7. The vendor shall provide vulnerability and configuration scan results to the Government on a monthly basis. The vendor shall provide raw scan results and administrative reports no later than the tenth (10^{th}) calendar day of each month.

5.8. The vendor shall close all discovered vulnerabilities within three (3) months of discovery, or provide a POA&M describing how they will work to close the vulnerability.

5.9. The vendor shall submit to the Government for approval, all mitigation plans that addresses any open vulnerabilities.

5.10. The vendor shall review all required policies, plans, and procedures documentation on an annual basis and submit changes to the Government for approval.

5.11. The vendor shall use the Government-approved method for remote access administration (DISA B2B) of the system or device.

Appendix A: Cybersecurity Regulations and Guidance

1) **Cybersecurity Regulations and Guidance**
The vendor shall use and comply with the most recent published versions of the following references, as well as all regulations or guidance referenced within those publications:

(a) United States Law
- (i) The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- (ii) The Federal Information Security Management Act (FISMA)
- (iii) The E-Government Act of 2002

(b) Office of Management and Budget (OMB)
The following publications are located at https://www.whitehouse.gov/omb/agency/default
- (i) Circular A-130
- (ii) Guidance M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Vendors

(c) National Institute of Standards and Technology (NIST)
The following publications are located at http://www.nist.gov/publication-portal.cfm
- (i) NIST Special Publication (SP) 800-37 – Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems
- (ii) NIST SP 800-39—Managing Information Security Risk: Organization, Mission and Information System View
- (iii) NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- (iv) NIST SP 800-60—Volume 1 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories

(d) Federal Information Processing Standards (FIPS)
The following publications are located at http://www.nist.gov/itl/fipscurrent.cfm
- (i) FIPS Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules
- (ii) FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems
- (iii) FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems
- (iv) FIPS PUB 201-2, Personal Identity Verification of Federal Employees and Vendors

(e) Department of Defense (DoD)
The following publications are located at http://www.dtic.mil/whs/directives/
- (i) DoD Instruction 5200.2, DoD Personnel Security Program (PSP)
- (ii) DoD Instruction 8500.1, Cybersecurity

(iii) DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
(iv) DoD Instruction 8510.01, Risk Management Framework Process (RMF)
(v) DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM)
(vi) DoD Instruction 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs
(vii) DoD Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs
(viii) DoD Directive 5400.11, DoD Privacy Program