Attachment 3

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

(f) The following publications are located at https://home.facilities.health.mil/low-voltage-system.
(i) DHA PM Standard Isolation Architecture for Cybersecurity of FRCS
(ii) Security Categorization for Facility-Related Control Systems (FRCS)
(iii) Facility-Related Control Systems (FRCS) Overlay
(iv) Standard Operating Procedure (SOP) for Facility-Related Control Systems (FRCS) Assessments
(v) Guidance for Facility-Related Control Systems (FRCS) Continuous Monitoring