Additional Questions and Answers

Translation and Interpretation Services at Brooke Army Medical Center (BAMC)

RFP# W81K0026RA042

11 August 2026

Please see the information provided below into the questions referencing Attachment 4, DHA Cybersecurity RFM Requirements.

Q&A Item	Government Response in Q&A dated 7 August 2026	Actual "Attachment 4" Guidance	Alignment Assessment
Question 41 *(Does the ATO need to cover the exact version/configuration?)*	"The authorization has to cover the product and all its potential capabilities as deployed... a CBS [Cloud Broker Services] question is a cloud service."	Section B.1.11 & B.1.12 require the delivered device/system to match the "DoD authorized configuration" and require an ATO/APL on "all equipment/product versions." Section A.1.1 mandates reporting *any* software, OS, or component changes.	Highly Aligned. The Government is correct. Attachment 4 leaves no room for generic or outdated approvals; any change to the deployment, version, or configuration triggers a re-evaluation.
Question 42 *(What are the Nessus scanning/boundary details for SaaS?)*	"You can't theoretically derive an architecture diagram or authorization boundary... Assessment will require all of these items..."	Section B.1.1 explicitly mandates a "fully-credentialed NESSUS scan with RFO submission" and monthly scans post-award. Section B.1.4 sets hard limits (zero unmitigated high/moderate vulnerabilities).	Highly Aligned. The Government correctly notes that these boundaries are "tangible" and "fully-fleshed out" during the assessment. Attachment 4 confirms that these technical parameters (Nessus scans, STIG compliance) are hard, non-negotiable requirements to obtain and maintain an ATO.
Question 43 *(Do these medical device rules apply to a remote SaaS?)*	TBD	The document is titled "DHA Cyber Logistics (CyberLOG) Cybersecurity..." and refers broadly to "New	The rules do apply to SaaS. Because the SaaS platform is accessed via browser on DHA networks, it must still

		Equipment/Product systems, equipment and software" (Section A.1). It governs *any* IT product interacting with DHA networks.	be assessed to ensure no vulnerabilities compromise the endpoint.

Further details:

The DHA Cloud Governance Framework (CBS & ESA-BAD)

When the government response mentions that *"largely a CBS question is a cloud service"* and that boundaries are *"fully fleshed out during the ESA-BAD/CBS assessment,"* they are referring to the formal DHA vetting process for cloud products.

DHA entity	Role in your Procurement	How it relates to Attachment 4
CBS *(Cloud Broker Services)*	Acts as the mandatory gateway and broker for any cloud service (SaaS, PaaS, IaaS) entering the DHA environment.	Section B.1.12 (maintaining an ATO) and Section B.1.1 (Nessus scans) are processed through CBS templates and tools to ensure the cloud boundary is secure.
ESA-BAD *(Enterprise Service Association)*	Conducts the actual security assessments, technical reviews, and risk determinations for the platform.	This is the body that will physically verify the Nessus scans required by Section B.1.1 and the STIG compliance required by Section B.1.4.