DHA CIO Meeting with Industry

AMSUS-SM Technology WG and The Coalition for Government Procurement

August 10, 2022

ATO Process

1. When is the RMF process applied and how proactive can companies be in the process (when does it apply in the contracting process)?
2. What is MITRE's role in the current process?
3. Are there any specific ATO processes to address recalls?
    a. What is the cybersecurity use policy for medical devices under Class I Medical Device recalls and remediation requiring new FDA 510(k) clearance?
    b. Is there an expedited cyberlog ATO procedure to ensure patient safety when a medical device is recalled and requires to be replaced by a new medical device?
4. Is there an escalation path that contractors can follow if an RMF process extends beyond the recommended timeframe?
5. Who covers the cost of achieving an ATO, can the vendor charge to cover the ATO costs or should it be a vendor expense?
6. When a product has received an ATO certification, what should vendors do next? What do contractors need to provide to a site to confirm that a product has received the ATO certification?

Training and Resources

7. Is there a flowchart of the ATO process (and checklist) available that industry can reference as they prepare to submit a product for an ATO?
8. Is there a publicly available resource that industry (and perhaps clinicians and others within DHA) can reference that describes the products that require an ATO (and those that do not)?
9. Does DHA post training or other resources publicly for vendors to understand the expectations of the Government during the ATO process?
10. Is training and/or resources provided that covers new ATO requirements or major changes?
11. Does DHA train its contracting officers to know when an ATO is required and when it is not?
12. During the last meeting, the DHA shared a new DHA Assess and Use Guide—can DHA provide what the process will look like for those products?
13. Is there a central phone or email address that contractors can direct questions to?

14. Are there any questions (or issues) that DHA consistently receives from industry during the ATO process that we can assist in clarifying with our member companies?

Harmonization of ATO Criteria with Other Agency Requirements

15. Can DHA share how the Government will utilize the theory of "reciprocity" of the certifications? Is there any more information on this process, especially between the DoD and VA? Both have their own "risk assessment" processes and greater consistency will help contractors complete the VA 6550 Appendix A requirement and remove overhead on duplicative processes.
16. Is an ATO certification for DHA recognized by the VA and/or other agencies?
17. Could DHA provide an update on an Enterprise ATO and JAB (FedRAMP) versus a facility level ATO?
18. With the FDA updating its cybersecurity guidance, are there any efforts by DHA and FDA to harmonize any of their respective criteria/requirements?
19. Do DHA ATO cybersecurity policies align with FDA 510(k) safe patient use policy?
20. Does DHA cyberlog require a valid medical device FDA 510(k) clearance certificate as a minimum prerequisite for cybersecurity evaluation and accreditation?

In Closing

21. What can industry do to be a better partner with DHA in ensuring that commercial medical products and other healthcare technologies are secure?