RMF ATO – (A&A) and EAL Certification

Scenario:

Company X wants to certify a Crypto module with concurrent certifications, Government ATO - A&A, and an EAL 7 certification. How would you accomplish these goals within roughly the same time frame?

Response:

Since both the EAL 7 certification and the ATO or "Authorization to Operate" (NIST, 2010) A&A "Assessment and Authorization" (U.S. Department of the Interior, n.d.), require similar proof/evidence regarding the security and soundness of the entire SDLC, performing both certifications concurrently will likely save time in the long run, although I would recommend finishing the EAL 7 certification first (NIST, 2010; Ouyang, n.d.). To that point, many of the formal design requirements of EAL 7 can be included in the Security plan portion of the ATO assessment (NIST, 2010; Ouyang, n.d.). Moreover, since the formal testing and verification requirements of EAL 7 require that there be no errors in the product/TOE, achieving an EAL 7 rating and including said EAL 7 rating in the "Security assessment report" (NIST, 2010) portion of the ATO assessment will fulfill many of the requirements of that document (NIST, 2010; Ouyang, n.d.). Moreover, the POA&M or "plan of action and milestones" (NIST, 2010) section of the ATO assessment will be limited as the system will be proven to be error-free by achieving an EAL 7 rating before ATO A&A (NIST, 2010; Ouyang, n.d.; UMGC, 2022). Lastly, an EAL 7-rated crypto module will necessarily meet the ATO standards, as the "Federal Information Processing Standard (FIPS) 140-2" (Evans et al., 2001) highest security standard is "Level 4" (Evans et al., 2001) which only requires "CC evaluation assurance level EAL4" (Evans et al., 2001).

References:

Evans, D., Bond, P., & Bement, A. (2001). *FIPS PUB 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

NIST. (2010, February). *Guide for Applying the Risk Management Framework to Federal Information Systems*. Login.microsoftonline.com. https://learn.umgc.edu/content/enforced/111374-022073-01-2158-GO1-9040/sp800-37-rev1-final.pdf?_&d2lSessionVal=blYuJSGR0zpBLApxbqVDD9Vyf&ou=214866&ou=930353

Ouyang, A. (n.d.). *CISSP ® Common Body of Knowledge Review: Security Architecture & Design Domain*. Retrieved February 17, 2024, from https://opensecuritytraining.info/CISSP-2-SAD_files/2-Security_Architecture+Design.pdf

U.S. Department of the Interior. (n.d.). *DOI Security Assessment & Authorization*. Www.doi.gov. Retrieved February 18, 2024, from https://www.doi.gov/ocio/customers/assessment

UMGC. (2022). *Session 3 Notes*. Learn.umgc. https://learn.umgc.edu/d2l/le/content/930353/viewContent/32137750/View