September 09, 2024

Federal Risk and Authorization Management Program
General Services Administration
1800 F Street, NW Suite 400
Washington DC, 20405

Submitted electronically via fedramp.gov

Re: FedRAMP Proposed Policy Update on the Application of Federal Cryptography Standards

The Cloud Service Providers-Advisory Board (CSP-AB) welcomes the opportunity to respond to the proposed policy update ('the Proposal') to how the Federal Risk and Authorization Management Program (FedRAMP) applies federal cryptography standards to cloud providers that participate in FedRAMP.

The CSP-AB represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them. Collectively, our members hold over 700 authorizations to operate (ATOs) across all service models and impact levels, and adhere to U.S. Government FedRAMP requirements.

The CSP-AB is highly supportive of the Proposal. In particular:

- We agree that a risk-based approach is required, as the validation of a cryptographic module (e.g., FIPS 140 validation) should not overshadow the broader security context. This approach is essential given that validated modules might still have known vulnerabilities that could pose significant risks.
- The Proposal correctly highlights situations where unvalidated modules may be preferable, especially when validated modules have known vulnerabilities. This flexibility will enable hyperscale cloud technology for the wider government industry, and allows for more practical and secure decision-making in rapidly evolving technological environments. However, we would like to see the requirements related to the justification of using non-validated modules to expand beyond solely security issues.
- The Proposal strikes, in our view, the right balance between the need for compliance with federal standards (such as FIPS) and the practical realities of modern cloud environments. By allowing for the use of unvalidated modules under certain conditions, FedRAMP will promote a more dynamic and responsive approach to security.
- The CSP-AB is supportive that regular re-evaluation and transparency are central to the Proposal, as this will ensure security practices remain agile, relevant and effective as threats and technologies evolve.

- We consider the implementation date of January 01, 2025 to be sufficient to allow stakeholders sufficient time to align their practices with the new requirements.

However, we are concerned that the Cryptographic Module Validation Process (CVMP) is still insufficient. For example, regarding CSP02 ("CSPs shall accurately document in Appendix Q of their SSP all cryptographic use cases and modules and module versions in use"), this is not a feasible expectation of any hyperscale cloud where cryptography is used throughout its products. Such a list would be immediately inaccurate and/or incomplete and it's not clear what benefit it will provide the FedRAMP program.

While we appreciate that NIST is reviewing the CVMP, our members are still experiencing unacceptable delays in securing the testing and validation of updated cryptographic modules. This in turn impacts what CSPs are able to offer the Federal government, running contrary to FedRAMP's 'security first' mantra.

We thank you for your consideration of our comments and the CSP-AB stands ready to serve as a resource as FedRAMP continues to refine the proposed metrics.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

lnavaratnam@csp-ab.com

http://csp-ab.com