Cybersecurity Coalition

Position on Cloud Security

The Cybersecurity Coalition submits the following position paper to address issue area #2 – *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government* and issue area #3 – *Guidelines outlining security measures that shall be applied to the federal government's use of critical software.* Additionally, this position paper may touch on the other issue areas outlined by NIST, including critical software in the cloud and specific requirements around the testing and provenance determination of critical software.

The recent Executive Order on Improving the Nation's Cybersecurity directs agencies to accelerate movement to secure cloud services. Given the increasing importance of cloud capabilities and the likelihood that some of these services will be considered "critical software", the Cybersecurity Coalition believes that the Federal Risk and Authorization Management Program (FedRAMP) must be incorporated throughout NIST's discussions on the criteria for designating "critical software", secure software development lifecycle best practices, and guidelines outlining required security measures.

As the Center for Cybersecurity Policy and Law notes in its Future of FedRAMP paper, *"Cloud computing emerged…as an important component of IT modernization, and FedRAMP has been an essential enabler of federal cloud adoption. Using standardization, testing, and risk management principles as part of the cloud service procurement process, FedRAMP has demonstrated what a thoughtful and well-run government program can achieve in the foundational areas of security, scalability, and automation.*"[1] The paper goes on to note the need for many areas of modernization that include several outlined in the recent Executive Order on Improving the Nation's Cybersecurity.

Providing agencies with guidance and guidelines around critical software, especially when much of the new critical software is cloud based, requires NIST to weave in the role that the FedRAMP program and its underlying baselines and processes must play in the determining the best way to secure critical software developed or deployed in cloud environments.

That said, FedRAMP has also been tasked with beginning work on several updates outlined in the executive order, including *"identifying relevant compliance frameworks, mapping those frameworks onto requirements in the FedRAMP authorization process, and allowing those*

---

1 https://static1.squarespace.com/static/5acbb666f407b432519ab15e/t/5e4fd3bf54725e7ce0483940/1582289857151/20-120+Cybersecurity+-+FedRAMP+brochure.pdf

frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate."[2]

The Cybersecurity Coalition strongly urges NIST to include both government and industry representatives to speak about the structure, requirements, and modernization efforts that FedRAMP provides to agencies during the conversation about the above topics. These representatives can also highlight leading security measures that critical software developers and operators should consider (e.g. defense in depth, segmentation, etc). In this vein, the Cybersecurity Coalition recommends John Banghart from Venable who works with the Cybersecurity Coalition.

Contact Info: Please reach out to Ross Nodurft (RBNodurft@venable.com) and Bri Law (BLaw@venable.com) for follow up on panels.

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/