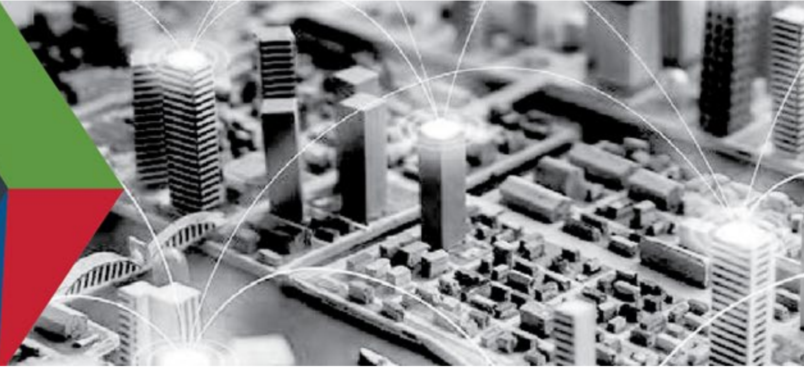
DEFEND TODAY, SECURE TOMORROW



Response to Comments on Cloud Security Technical Reference Architecture (TRA)

Introduction

On September 7th, 2021, The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the United States Digital Service (USDS), and the Federal Risk and Authorization Management Program (FedRAMP), released the Cloud Security Technical Reference Architecture (TRA) for public comments in accordance with Section 3(c)(ii) of the Executive Order 14028. Since the close of the comment period on October 1st, CISA, USDS and FedRAMP have reviewed and adjudicated comments from multiple stakeholders.

As the Federal government continues to migrate to the cloud, it is paramount that agencies implement data protection measures. The Cloud Security TRA will guide agencies as they securely migrate to the cloud by illustrating considerations for shared services, cloud migration, and cloud security posture management.

The Cloud Security TRA provides guidance on:

- The shared risk model for cloud service adoption (authored by FedRAMP).
- How agencies can build and maintain different cloud environments (authored by USDS).
- How to monitor such an environment through robust cloud security posture management (authored by CISA).

CISA wants to thank all commenters for the critical feedback and questions that allow the guidance documentation to be more effective for each federal agency. CISA reviewed and adjudicated stakeholder comments from the Request for Comments (RFC) period. The comprehensive review inspired further developments of the Cloud Security TRA.

The feedback is crucial to ensure the guidance fully addresses security considerations for the modernized protocol related to agencies' Cloud implementation. The input allows CISA to understand how the guidance needs to be developed to apply to all federal agencies broadly.

CISA considered each comment independent of the commenter and organization. CISA collaborated with USDS, and FedRAMP to understand the feedback, determine how to modify the Cloud Security TRA, and apply the changes appropriately to the documents. CISA identified themes from the collected comments and applied them to areas within the documentation that would improve the application of guidance to agencies and service providers.

Comment Themes

Overall, CISA, USDS, and FedRAMP highlighted six key themes from the comments and responses for all documents. Commenters wanted further clarification on or a better understanding of the following topics.

OMB Zero Trust Alignment

Commenters requested more alignment with OMB M-22-09 Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture. As a result, authors of the Cloud Security TRA updated the document to reflect the consistent use of Phishing Resistant Multi-Factor Authentication, reference to Centralized Identity Action, and additional logging requirements.

Topic Specific Details

Commenters requested more consistency in the use of the federal government's Identity, Credentials, and Access Management (FICAM) and highlighted considerations associated with Microservices. Authors of the Cloud Security TRA recognized the need to align with the FICAM Architecture and updated language throughout the document. Authors of the Cloud Security TRA also expanded application program interfaces (API) subsection with attention to Cloud-Native Authentication and Authorization and new scenario on Microservices and Service Mesh.

Commenters also noted a narrowing of how Zero Trust can be achieved in the text compared with National Institute of Standards and Technology (NIST) SP 800-207. Authors of the Cloud Security TRA updated the document to align with the NIST SP 800-207 guidance.

FedRAMP Program

Commenters requested clarity around certain aspects of FedRAMP, including policy, applicability, and direction of the program. Authors of the Cloud Security TRA conducted various updates to program scope and policy requirements, FedRAMP's intention around modernization and automation, guidance around training and use of FedRAMP templates, authorization boundary definition, potential use of governance, risk, and compliance (GRCs) within agency customers, and references to FedRAMP multi-agency Continuous Monitoring and Performance Management Guides.

Cloud Migration Strategy

Commenters sought a clarification on cloud migration strategies. Authors of the Cloud Security TRA updated Section 4.2.3 to provide a scenario showing why organizations should not move an application to the Cloud and add language to pursue the Refactor after the Rehosting is complete.

CSPM Capabilities

Comments requested additional guidance on internal coordination with CISA Programs such as Continuous Diagnostics and Monitoring (CDM), for scope of Cloud Security Posture Management (CSPM). However, the authors of the Cloud Security TRA purposefully took a wide aperture with the term in the document. In response to Executive Order 14028 and OMB Memo 22-09, the CDM Program Management Office (PMO) is starting to develop and test new cloud-specific requirements within the cloud. CSPM requirements are currently in the developmental phase and are in conjunction with the Cloud Security TRA. The authors also updated subsection in 5.3 to include explicit call outs to the relevant CSPM capabilities.

Requests for More Detail

Commenters requested more details and guidance on a variety of topics. Commenters requested more details and guidance on a variety of topics. Due to time and resource constraints, the authors of the Cloud Security TRA picked three topic areas and created short scenarios to accompany the main document via an appendix. These included Federated Identity Management, Microservices, and a Cloud-based Warm Standby.

Conclusion

CISA anticipates the Cloud Security TRA will better address stakeholder needs and concerns. The guidance is expected to evolve to reflect technological advancements and changes in threats to help ensure its usefulness to federal agencies. CISA is committed to supporting agencies and continuously receiving feedback to aid in developing future iterations of Cloud Security guidance.