FedRAMP ACQUISITION FAQS

Version 1

SEPTEMBER 26, 2017

FedRAMP

ACQUISITIONS FREQUENTLY ASKED QUESTIONS

In an effort to help agencies continue to adopt secure cloud technologies, FedRAMP has been identifying ways to create standard contract language that agencies can use in their acquisition process as they procure cloud-based products. In support of this effort, the FedRAMP PMO worked with OMB to develop this FAQ resource that agencies can reference when developing their solicitations. These FAQs are based on questions FedRAMP regularly receives from both vendors and agencies about how FedRAMP language can best be incorporated into RFIs, RFQs and RFPs.

QUESTIONS	ANSWERS
Can an Agency require a CSP to have a JAB P-ATO in a request for proposal?	No. Agencies cannot require a JAB P-ATO as a requirement to bid on a Federal contract. Federal agencies cannot include a JAB P-ATO as a condition of the contract as no agency can commit the JAB to issuing a P-ATO.
How can an agency show preference for a JAB P-ATO with respect to FedRAMP Authorizations when developing criteria for Offeror evaluations?	Program offices seeking to expedite the FedRAMP authorization can consider source selection criteria that can be used in evaluating offerors that may already have a JAB-P-ATO. Inclusion of such evaluation criteria should be discussed with the agency acquisition IPT, including appropriate legal representation.
Do FedRAMP requirements apply even if they are not included in a contract?	FedRAMP requirements apply to all Federal agencies when Federal information is collected, maintained, processed, disseminated, or disposed of by cloud service providers. Federal agencies are responsible for ensuring the FedRAMP requirements are met. Contractors are held accountable for performance written into a contract. Program and project managers must include FedRAMP requirements in performance criteria, deliverables, and other appropriate performance outcomes to facilitate inclusion in contract awards.
Is a FISMA ATO sufficient to meet FedRAMP requirements?	No. The FedRAMP process builds on the NIST FISMA baseline controls by removing requirements that are not applicable to commercial entities and replacing those with controls more appropriate for ensuring security related to protecting information maintained on behalf of the Federal government.
If a CSP is “FedRAMP ready”, is this an indicator that they will have an easier time getting through the FedRAMP ATO process?	Perhaps. FedRAMP ready means a CSP has expressed an interest in becoming a Federal provider by sharing information with the Federal government that indicates they can meet several of the baseline FedRAMP criteria. FedRAMP Ready does not mean the vendor has achieved a FedRAMP Authorization via the JAB or an Agency.

Can an Agency require a FedRAMP Authorization as a condition of the contract award?	In some cases, but only if there are an adequate number of vendors to allow for effective competition. Inclusion of FedRAMP authorization as a condition of contract award or use as an evaluation factor should be discussed with the agency acquisition IPT, including appropriate legal representation.
Can an Agency include specific data location requirements in a contract, such as CONUS only?	Yes. If an Agency has constraints and/or requirements for specific data locations (e.g., data-at-rest), the Agency should make those specific requirements known through the solicitation process. While FedRAMP does not provide or specify data location requirements, other Federal statutes, regulations, or policies may.
Is a Federal agency limited to only including FedRAMP requirements in a CSP contract?	No. Federal agencies have the responsibility and discretion to include any requirements necessary to protect information. FedRAMP sets a baseline for protecting Federal information in a cloud environment.
What does FedRAMP require for personnel screening requirements from CSPs?	FedRAMP requires CSPs to describe their organization's personnel screening requirements. If the agency has requirements for Federal background investigations or additional screening and/or citizenship and physical location (e.g., US citizens in CONUS offices only) then those requirements would need to be specified in the solicitation language, which may affect bid pricing.