AT-AT RFW

Government Responses to Industry

(queries submitted by January 10, 2018 at 3 PM ET)

1. PROGRAM AND SYSTEM-LEVEL QUERIES

1.1. Are you looking for a custom cloud solution that is hosted within DDS data centers or are you planning to use a public cloud service (like AWS GovCloud)?

Answer: DDS is seeking custom development of a software application (a provisioning tool) that will provide identity and account management, billing information tracking, access control, security and billing policy compliance, and request lifecycle management for cloud services to be procured under a separate effort. Hosting for this tool has not been determined.

1.2. How independent of a particular cloud provider do you want this system to be? Do you need a multi-cloud or hybrid-cloud capable solution?

Answer: Completely independent. The system should be flexible enough to support any cloud provider software that supports API access.

1.3. Does the Cloud Provisioning Tool need to support isolated CSP regions (ex: AWS GovCloud, AWS C2S)?

Answer: Specific CSP region support is not defined at this time.

1.4. Which CSPs do you wish to have this Cloud Provisioning Tool support? Is the intent to support multiple cloud server providers simultaneously? If so, will a given DoD organization, and/or even a given project within that organization, potentially use multiple CSPs simultaneously/in tandem?

Answer: Usage and identification of the Cloud Service Provider will be determined by a separate, parallel cloud services procurement effort by the DoD.

1.5. What are the typical use cases for this cloud? What types of teams within DoD would use this and which teams would not?

Answer: This tool will provide cloud provisioning support for all DoD agencies and Service branches. Refer to the Statement of Need for high level requirements of this tool.

1.6. What are the DevOps demands of this platform beyond provisioning of accounts?

Answer: Specific developer operations capabilities provided to DoD agencies and services will be fully fleshed out during user research. This project will use an iterative development approach that will force these difficult questions and integrations early in order to address risk quickly, fail fast, and pivot as necessary.

1.7. Is usability a concern or do existing cloud interfaces like AWS, Rackspace, or Google Cloud suffice?

Answer: User experience is a concern for all software applications. This project will be no different and will require user research and design to create the best UX possible for the tool.

1.8. Do you anticipate needing ongoing maintenance and support services or will you self-maintain the provided solution? If the latter, what are your preferred languages and platforms?

Answer: This effort is for the development of a prototype software solution that will provide the minimum requirements for a system described in the Statement of Need.

1.9. Do you anticipate any additional integrations that may be desired down the road, after this original scope is complete?

Answer: This tool will be developed using an iterative approach. We cannot anticipate how the requirements may change at this point. The integrations identified in the Statement of Need are what is currently identified.

1.10. How custom of a solution do you need? What general capabilities would DDS need in the account provisioning process or in the self-service tools?

Answer: Please see Statement of Need. This tool will be developed using an iterative approach. All capabilities will be fleshed out as they are tackled in the development lifecycle.

1.11. How many users will the AT-AT prototype support? What are the estimated initial number of CSP Accounts and Aggregate Spending that the Cloud Provisioning Tool would need to manage?

Answer: Number of users and spending will be determined by a separate cloud services procurement and the phased migration of systems.

1.12. Will this system be classified? At what level?

Answer: Development will be done completely unclassified and must be deployable to all classification levels.

1.13. Do you expect any push-style alerting requirements?

Answer: Low-level functionality such as this will be determined by user research and through iterative development.

1.14. Is there an existing system that provides the existing capability? If so, can you provide any as built documentation (e.g., user guide, architecture)?

Answer: There is not.

1.15. Can best-in-class open source and commercial solutions be used over US Government standards?

Answer: Yes, if the solutions meet the desired functionality requested in the Statement of Need and can be proven to be a secure, stable, and viable component of a larger system.

1.16. How does the government intend on procuring the Cloud Provisioning Tool and CSP Services?

Answer: The provisioning tool being requested with this Statement of Need will be acquired using a Commercial Solutions Opening (CSO) using Other Transaction Authority (OTA), a non-FAR based acquisition authority provided under 10 USC 2371(b). Cloud services procurement is a separate effort.

1.17. What Government organizations will the awarded vendor have to interface with?

Answer: This project will be managed by the Defense Digital Service (DDS), an agency within the Department of Defense. No other government organizations have been identified at this time. System level integrations are detailed below.

1.18. What is your timeframe for deployment?

Answer: Project kick off is expected the first week of March 2018 with MVP delivery scheduled for late FY18. Specific project milestones will be established upon kickoff.

2. System Integration

2.1. What specific DoD Systems are envisioned to integrate with the Cloud Provisioning Tool?

Answer: Specific integration points have not yet been determined. The system must be able to connect with specified DoD identity and financial systems as well as CSP APIs. This includes programmatic access as well as person access, with both Common Access Card (CAC)/Public Key Infrastructure (PKI) authentication as well as standard multi-factor authentication. This project will use an iterative development approach that will force these difficult questions and integrations early in order to address risk quickly, fail fast, and pivot as necessary.

2.2. Will an existing DoD system handle multi-factor authorization or is that part of the remit of this engagement? Can you please provide more detail on what you mean by "as well as standard multi-factor authentication"?

Answer: The specific system level integrations have not yet been determined. This project will use an iterative development approach that will force these difficult questions and integrations early in order to address risk quickly, fail fast, and pivot as necessary.

2.3. Will HTTPS certificates utilized on deployed systems come from the DOD PKI or from a commercial provider?

Answer: Specifics around SSL certificates have not been determined.

2.4. The statement of need refers to "programmatic access" to "DoD identity and financial systems" -- do the services in question provide HTTP APIs (eg REST JSON/XML) or will access be via some other protocol / standard? How is programmatic access to those services managed (eg OAuth or OAuth-like access tokens? Signed JWT-like tokens? Stored usernames/passwords? Other?)

Answer: There may be a need to create API middleware as necessary to connect this tool to DoD financial and identity systems which may use non-industry-standard formats or protocols.

2.5. Based on the statement of need it would appear that access to billing systems is to be for reporting purposes only. Can you confirm this to be true or do you expect this system to interface with a payment provider and take payments itself rather than acting as a proxy for the actual cloud service provider for any billable action (e.g. spawning a new VM, resource pool or service)

Answer: This system will be integrated with DoD financial systems as determined necessary to facilitate payment and connection to CSP billing systems. Precise payment mechanisms will not be known until the completion of a separate cloud services procurement.

3. SECURITY AND CONFIGURATION

3.1. Is the tool intended to actually establish and initiate the desired CSP environment itself, programmatically? If so, given that a very broad variety of IaaS and PaaS environments, tools, and frameworks are available -- e.g. serverless computing, deep learning tensor processing, natural language processing, etc. -- will this service manager only handle a fixed, standard subset of IaaS / PaaS platforms? Or is it intended to support the entire panoply of what's available, and grow as new CSP features / offerings are made available?

Answer: Yes the panoply of what's available is in scope, as technically feasible. However, this project will use an iterative development approach that will flesh out these details quickly to identify specific use cases and user stories.

3.2. With reference to "auditing accounts" -- will the system require a deep audit trail (i.e. every action taken by every user is logged) or a relatively shallow one (i.e. only actual finalized transactions are logged)?

Answer: Specific logging requirements have yet to be determined, however the requirement will extend beyond finalized transactions.

3.3. Do you anticipate mandating row-level or cell-level security on any storage systems utilized?

Answer: Such a requirement has not be determined. However, this project will use an iterative development approach that will flesh out these details quickly to identify specific use cases and needs.

3.4. Do you require a headless API for scripted interaction with the developed system? (e.g. will a third-party company or DoD agency/department be managing said system and will they require the ability to do so via Scripts instead of a traditional login via the browser)

Answer: Specific requirements for the system's back end are not defined to a level that would strictly require such a design approach. However, a well defined and documented back end API is in line with modern software development practices.

3.5. Outside of policies to ensure FedRAMP compliance, what additional security policies are envisioned that the Cloud Provisioning Tool would need to apply?

Answer: DoD specific “Above and Beyond” FedRAMP compliance controls will apply. Data will be across classification levels (UNCLASS/FOUO/CUI/SECRET/TS) and commensurate security considerations may apply. Additional security measures may be defined at a later date but generally industry best practices will apply. Note that development will occur in an unclassified environment.

3.6. What specific levels of compliance does the Cloud Provisioning Tool need to be accredited under (ex: DoD SRG)?

Answer: Specific compliance levels are still being determined.