dlt.com

BRIEFING

Civilian Market
Update: Cloud Smart Strategy

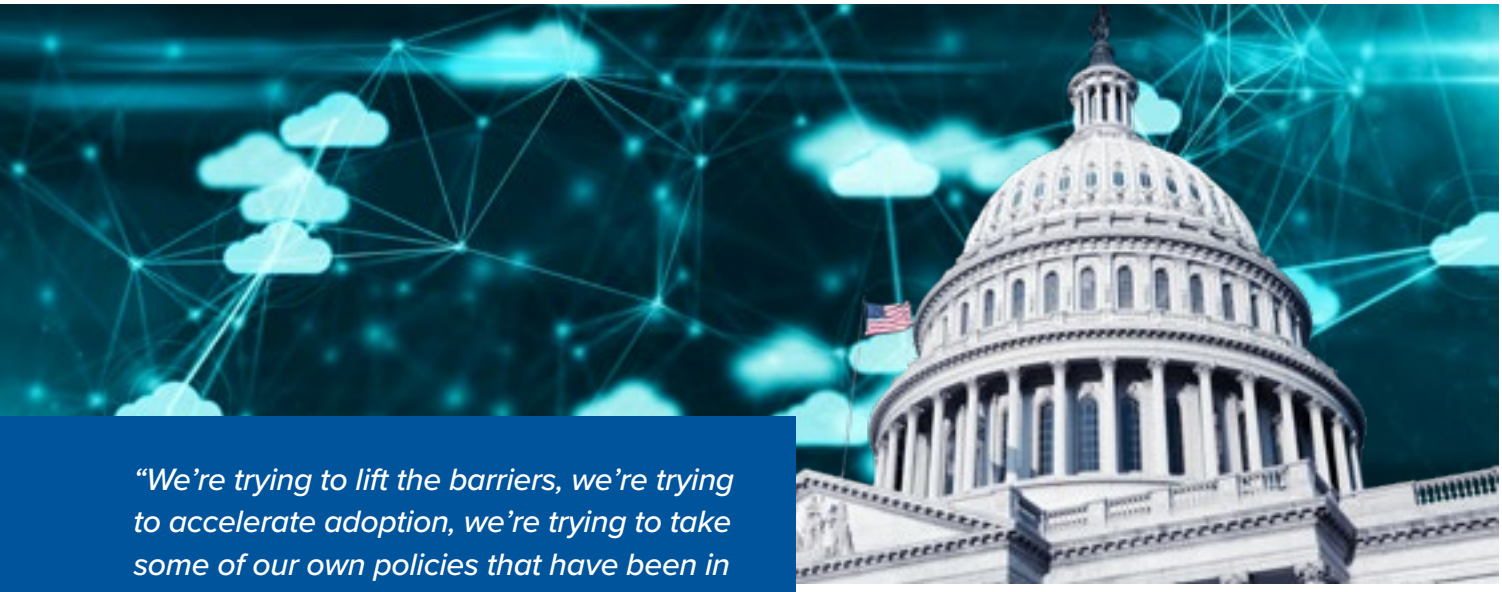
Louis Dorsey
Senior Director, Civilian Strategic Markets

DLT®

Accelerating Public Sector Growth for Technology Companies

September 2019

CLOUD SMART STRATEGY: WHAT YOU NEED TO KNOW



"We're trying to lift the barriers, we're trying to accelerate adoption, we're trying to take some of our own policies that have been in place for multiple years and change those so that we can actually move forward."
—Margie Graves, Federal Deputy CIO

The finalized version of Suzette Kent's Cloud Smart Strategy was released in June 2019 by the Office of Management and Budget (OMB). The original blueprint of the Cloud Smart draft plan was introduced in September 2018, which was a summary of the federal agency's 2011 "cloud adoption strategy," where they released their first guidance publication of the "cloud first" initiative. The final version is meant to be a "practical implementation guidance," helping government agencies "fully actualize the promise and potential of cloud-based technologies while ensuring thoughtful execution that incorporates practical realities" as stated by Margie Graves, Federal Deputy CIO at a FedScoop Cloud Talks industry event. Of the 22 "action items" set forth by the Federal CIO Council to be accomplished over the coming months, over half of them have already been completed.

Graves' major theme for the Cloud Smart Strategy is the level of flexibility it gives agencies to craft their own individual cloud adoption journeys. Cloud Smart also empowers agencies to decide which applications they feel are well-suited for the cloud and which applications need to stay in their current infrastructure.

There are a few changes between the initial Cloud Smart draft and the final version. The major change is the emphasis on application rationalization. To help agencies with this decision, the Federal CIO Council and the government's Cloud & Infrastructure Community of Practice released the Application Rationalization Playbook guide, a six-step guide to "structured" IT portfolio management.

As in the Cloud Smart proposal, the final version is focused on three key pillars for successful cloud adoption: ***Security, Procurement and Workforce.***

I. SECURITY

This strategy strongly encourages agencies to take a risk management-based approach to securing their environments and emphasizing the President's Report on Federal IT Modernization recommendation of "data-

level protections and fully leveraging modern virtualized technologies." This in-depth strategy requires agencies emphasize protecting the data-layer in addition to the network and physical infrastructure layers.

Cloud Smart encourages agencies to approach security and privacy in terms of intended outcomes and capabilities. The major elements that must evolve in the federal security strategy as part of this outcome-driven approach are ***Trusted Internet Connections (TIC), Continuous Data Protection and Awareness and FedRAMP***.

TRUSTED INTERNET CONNECTIONS

The original concept of TICs was during a time when networking was confined by physical limitations, and network security was not standardized and served its purpose of protecting the network and data. Today, TICs are inflexible and incompatible with the requirements of most agencies. Technology has evolved to provide more tools and approaches to secure data. With the adoption of private-sector cloud offerings, software-defined networks (SDN), and the increase in mobile workforce, the TIC model must evolve and become more flexible to compete with other models that provide equal or greater security.

To address this, DHS is working on pilot agency-specific approaches to meet the original intent of the technical constraints of the one-size-fits all model. This newer approach will be incorporated into the TIC Reference Architecture and highlight use cases of security objectives that can be achieved without directing all traffic through pre-defined physical access points. In addition, it will show different use cases that do not require traffic to be routed through a TIC can address government-wide intrusion and detection efforts, like the EINSTEIN program, while maintaining DHS established controls to ensure a baseline level of security across the federal enterprise.

This approach will allow agencies to take advantage of new approaches, such as zero trust networks to manage risks.

CONTINUOUS DATA PROTECTION AND AWARENESS

In summary, Encryption & Identity, Credential, and Access Management (ICAM) implementation is essential and relevant, especially in cloud-based environments. Specifically, in situations where the agency is partnering with a service provider to manage network visibility and data protection.

Agencies are being encouraged to incorporate service level agreements (SLA) with all cloud service providers (CSP) to include access to, and use of, log data given. Each agency is the custodian of its information, which makes them responsible for the cloud-hosted data and ensuring it aligns with its ICAM systems. Furthermore, agencies need to be aware of the following:

- Whether their information will reside on third-party information systems prior to implementing an SLA.
- Agencies should have continuous access to log data.
- Agencies must be notified promptly of any cybersecurity incidents, breaches, or any other suspicious occurrences that involves any information or information systems covered by the SLA.

As more federal agencies adopt commercial cloud solutions, DHS's CDM program is continually being made aware of, and evaluating analytical tools and capabilities, that can scale across multi-cloud environments to facilitate continuous visibility and information sharing.

FEDRAMP

While FedRAMP has standardized the government's approach to security assessment, authorization and continuous monitoring of cloud services, there are still issues that need to be addressed. Some examples of these issues are:

- The lack of reciprocity across agencies to FedRAMP authorizations results in duplication of efforts when assessing security for product deployment.

CLOUD SMART STRATEGY:
WHAT YOU NEED TO KNOW

"Vendors and partners should be looking to frame their go-to-market strategy and messaging within the context of the Cloud Smart strategy. Be ready to articulate how your offering relates to the government's security needs, procurement methods and workforce reskilling."
—David Blankenhorn, DLT CTO

- Many agency specific processes make it difficult for agencies to issue Authorization to Operate (ATO) for solutions, even when using existing authorized CSPs.

There are several initiatives under development to address these challenges and improve the overall process and accelerate common ATO agreements. The intent of the initiatives being evaluated will do the following:

- Drive better and more automated control and monitoring.
- Prioritize the approach to control implementation.
- Normalize control use across the federal enterprise.

This will reestablish FedRAMP's role in the risk assessment process as a verification check for agencies when they make their cloud decisions, rather than today's cure-all for all matters related to implementation risks of a cloud solution.

II. PROCUREMENT

While some of the wide selection of recommended actions by industry, interagency working groups and individual agencies to accelerate the adoption of cloud solutions have been translated to federal-wide guidance, there is still a lack of consistency on agency implementations and information sharing on best practices. Without an all-encompassing guide, agencies struggle with searching across multiple sources to gain the basic understanding of the cloud services available in the commercial marketplace, the different offerings on existing government-wide acquisition contracts (GWAC) and the best way to evaluate which approach is best for their specific requirement.

To address these challenges, agencies will need a variety of approaches to leverage their buying power, the shared knowledge of good acquisition principles and relevant risk management practices. As part of the Cloud Smart multidisciplinary approach, agencies will need to do the following:

- Place security and privacy considerations at the

forefront of any procurement effort.

- Avoid vendor lock-in by evaluating the business process dependencies of any new solution.
- Update their business continuity and disaster recovery plans to include contingencies involving the sudden interruption or termination of service.

Other common practices to ensure cost-effective and safeguarded procurement of cloud-based solutions for federal procurement officials to consider are ***Category Management, Service Level Agreements and Security Requirements for Contracts***.

CATEGORY MANAGEMENT

Category management simplifies the process for industry to do business with the government by reducing duplicative contracts and decreasing costs for bids, proposals and contract administration. It also offers the federal government the opportunity to improve buying practices that support Cloud Smart strategies, increase adoption of proven cloud vehicles in the federal marketplace and develop new vehicles to address emerging demands Simply put, category management aims to:

- Deliver more savings, value and efficiency for agencies.
- Eliminate unnecessary redundant contracts.
- Meet the government's small business goals.

OMB has published a memorandum that provides guidance on category management implementation principles.

SERVICE LEVEL AGREEMENTS (SLAs)

Cloud Smart offers a two-track approach to smarter cloud purchasing and usage across Federal agencies through improvements to SLA use, as outlined below:

- Firstly, candidates for inclusion as standard clauses that apply to commercial items in the Federal Acquisition Regulations (FAR), including new SLAs, must generally meet at least one of the following criteria:
  - *The clause is required to implement a provision of law applicable to the acquisition of commercial items.*
  - *The clause is generally consistent with customary commercial practice.*
- Secondly, executive agency heads are accountable for managing the risks to their enterprises, even with respect to contractor-operated systems.

With these improvements to the effective use of SLAs in mind, there needs to be a government-wide review and selection of contractual terms and conditions specific to cloud-based commercial offerings that will be standardized across agencies. Standardizing cloud contract SLAs will provide 1) more effective, efficient and secure cloud procurement outcomes and 2) enable enhanced management of risk with greater consistency and transparency in negotiations with commercial CSPs. To facilitate effective risk management in the SLA, agencies should:

- Clearly articulate what services a CSP performs and at what level.
- Granularly establish roles and responsibilities.
- Establish clear performance metrics.
- Implement remediation plans for non-compliance situations.

This will ensure that services are performed as intended, with a proper SLA in place, and offer agencies a way to mitigate risks while optimizing the performance and efficiency of the cloud solution.

SECURITY REQUIREMENTS FOR CONTRACTS

The Federal CIO published an updated **High Value Asset (HVA) memorandum** that highlights considerations for managing risks across hybrid environments. This is essential as agencies consider the security and privacy risk to information and mission services when

CLOUD SMART STRATEGY:
WHAT YOU NEED TO KNOW

Agencies should identify potential skill gaps that emerge as a result of a transition to cloud-based services, and where needed, equip their existing staff with additional skills and knowledge.

making cloud procurement and deployment decisions. The guidance says agencies must now ensure that contracts impacting their HVAs include provisions that provide the agencies with continuous visibility of the asset. In addition, the guidance will strive to improve HVA trustworthiness by requiring developers, manufacturers and vendors to employ best practices for designing, deploying and securing systems.

III. WORKFORCE

As agencies adopt and migrate to cloud platforms, the impact that these migrations have on the federal workforce needs to be examined. Specifically, agencies should identify potential skill gaps that emerge as a result of a transition to cloud-based services, and where needed, equip their existing staff with additional skills and knowledge to keep up with the ever-expanding list of technology options available to procure and deploy. Some of the strategy's agencies are taking to transform their workforce are as follows:

- Development programs for emerging talent or future leaders.
- Apprenticeship programs.
- Initiatives to convert non-IT personnel where aptitudes align.
- Exchanges of qualified personnel through public-private partnerships or interagency detail opportunities.

The areas the government will specifically focus on to equip their existing staff and fill their skills gap are as follows:

- Identifying skill gaps for current and future work roles.
- Reskilling and retaining current federal employees.
- Recruiting and hiring to address skill gaps.
- Employee communication, engagement and transition strategies.
- Removing bureaucratic barriers to hiring talent expeditiously.

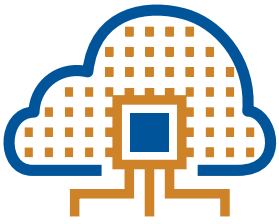
While federal agencies should continue to comply with the National Initiative for Cybersecurity Education (NICE) Framework to help standardize government-wide cybersecurity workforce gap assessments, they are encouraged to conduct their own enterprise-wide skills gap analysis to ensure inclusion of all current and future IT skills and positions specific to their workforce requirements.

FINAL THOUGHTS

The basic and primary focus of Cloud Smart is to equip agencies with the tools, knowledge and resources needed to make decisions that work for their specific agencies, rather than a one-size-fits-all approach.

By leveraging modern technologies and best practices, agencies will be in a much better position to take advantage of new capabilities while expanding existing capabilities to enable their missions and deliver services to the public.

Government agencies are going to move to a "solve before buy" rather that "buy before build" approach. In other words, agencies are going address their service needs, fundamental requirements, and gaps in their processes and skillsets before starting a new procurement. Industry partners need to know this beforehand and approach their agency customers about how they can assist them with this approach.



Written by Louis Dorsey
Senior Director, Civilian Strategic Markets

Questions?

Contact Us and Become Cloud Smart

Email: sales@dlt.com
Web: dlt.com/cloud

dlt.com

DLT®

Accelerating Public Sector Growth for Technology Companies