Federal Cloud Computing Strategy

This is a draft strategy open for public feedback. You may provide feedback in three ways:

1. Content suggestions and discussions are welcome via GitHub “issues.” Each issue is a conversation initiated by a member of the public. We encourage you to browse and join in on discussions in existing issues, or start a new conversation by opening a new issue.

2. Direct changes and line edits to the content may be submitted through a "pull request" by clicking "Edit this page" on any site page in the repository. You do not need to install any software to suggest a change. You can use GitHub's in-browser editor to edit files and submit a pull request for your changes to be merged into the document. Directions on how to submit a pull request can be found on GitHub. Open pull requests for the proposed guidance can be found in the site repository on GitHub.

3. Send your content suggestions or proposed revisions to the OMB Office of the Federal Chief Information Officer via email to ofcio@omb.eop.gov. Please note that all comments received will be posted publicly.

From Cloud First to Cloud Smart

To keep up with the Country’s current pace of innovation, this Administration has placed significant emphasis on utilizing IT modernization to improve the services the Federal Government provides to the American people. Through an Executive Order (EO), President Trump directed the creation of a report on the modernization of Federal IT. This report identified over 50 tasks that improve citizen-facing services, accessibility, and maintain cybersecurity.

In 2010, the Federal Government created the first cloud strategy, called Cloud First. This policy was created at a time when cloud technology was still relatively new, and provided agencies broad authority to adopt cloud-based solutions. However, absent an implementation plan or strategy, agencies were slow to adapt. While Cloud First successfully highlighted the importance of IT modernization efforts, its shortcomings needed to be addressed. This is why this Administration has developed Cloud Smart, a new strategy for agencies to adopt cloud solutions that streamline transformation and embrace modern capabilities. Cloud Smart focuses on equipping agencies with the tools needed to make informative technology decisions in accordance with their mission needs, and leverages private sector solutions to provide the best services to the American people.

Cloud Smart encompasses several key components of IT modernization including security, procurement, and workforce. Historically, policies have isolated these areas, creating confusion and a misunderstanding of requirements, mission, and needs. However, they are deeply linked, and require an integrated, interdisciplinary approach, rather than a one-size-fits-all approach to IT modernization. Cloud Smart combines these disciplines together into a cohesive strategy that provides savings, security, and faster delivery of mission-serving solutions.

Agencies will need to share their transformative experiences with their peers, so that Government can leverage collectively-gained knowledge. The ability to evaluate, consume, and share knowledge is the driver of success in private sector IT modernization efforts – the Federal Government’s approach should be no different. By investing in these capabilities now, agencies will ensure the best, and smartest, approach to serving missions and being stewards of taxpayer dollars.
Key Actions

The Chief Information Council and Chief Financial Officer Council will work with the Office of Management and Budget, the General Services Administration, the Department of Homeland Security, and other Federal agencies to develop a work plan of actions and targeted policy updates delivered over the next eighteen months to move the Cloud Smart agenda ahead. This plan will be technology-neutral, and will consider vendor-based solutions, agency-hosted solutions, inter- and intra-agency shared services, multi-cloud, and hybrid solutions as appropriate. For agencies to remain effective in the 21st century, these Cloud Smart actions will need to be iteratively reviewed and improved over time to keep up with the changing market and emerging technologies.

I. Cloud at a Glance

(Re-)Defining Cloud Computing

The term “cloud” inside of Government is often used to refer to any technology solution provided by an outside vendor. In practice, “cloud computing” refers to a variety of technologies that allow the rapid provisioning of systems or services from a shared pool of resources, ranging from hosted email solutions provided by a private company, to a scalable application container run on government-owned servers in a government-owned data center. A cloud migration strategy should not be considered a question of who owns the computing resources, data, and facility, but rather can this solution improve service delivery to citizens. Evaluating specific capabilities of services, such as automatic scalability, is useful when evaluating solutions, rather than just considering if an application is “cloud” or not.

Much of the previous guidance on the topic of cloud technology focused on potential benefits instead of realizing outcomes. As an example, moving an application from a traditional data center to a virtualized infrastructure vendor generally does not enable automatic application scalability with increased user demand. To achieve this goal, project development and execution efforts will often be needed to refactor applications to take advantage of new capabilities such as auto-provisioning and auto-scaling, and this must be factored into analysis and planning.

The traditional cloud deployment models reflected a progression of increasing vendor-ownership through system layers, from Infrastructure as a Service (IaaS) where vendors provide only the infrastructure and hardware, to Platform as a Service (PaaS) where vendors provide hosting and infrastructure management, to Software as a Service (SaaS) where agencies only need to provide their data and most other capabilities and functionality are provided by a vendor. Industry has since moved to a more finely differentiated set of capabilities at different layers. The rapid development of both open source and proprietary offerings have made possible today almost any combination of vendor and Government ownership of these various layers. Most major vendors now offer a variety of available adoption paths and services depending on end-user needs. Industries that are leading in technology innovation have also demonstrated that hybrid and multi-cloud environments can be effective and efficient.

Private industry now offers such a large range of possible solutions, and agencies must be properly equipped to evaluate the choices available to them based on their service and mission needs. Agencies should make computing and technology decisions that take into account end-user impact balanced against cost and risk management criteria.
Modernization and Maturity

Cloud technology adoption requires that agencies prioritize migration planning, sustainment, and organizational maturity in order to realize the full benefit of these services. One way in which adoptions fail is when organizations buy solutions without proper identification of requirements and intended outcomes. This can lead to a project not launching, a service failing at peak need, or simply redundant purchasing across the enterprise.

As technology changes, agency information technology strategies need to mature as well. Modernization is an ongoing commitment that is not sustained with single interventions once every decade. Rather, modernization is a constant state of change, and part of the day-to-day business of technology at every agency. To that end, policy, guidance, and requirements need to be iteratively improved to match changing needs, lead mature practices, and drive positive outcomes.

To accelerate cloud adoption, agencies should be expected to regularly evaluate their current state of maturity across the agency. Security, Procurement, and Workforce are three key areas that require serious consideration and investment to ensure successful adoption. Agencies should also evaluate their user needs for efficiency, accessibility, and privacy in the context of the solutions they choose.

For example, to utilize the distributed nature of cloud, moving security controls from the network perimeter closer to the data itself can improve the overall security posture. To realize the scalability, stability, security, and speed to market benefits of cloud infrastructure, agencies need to utilize modern agile development skills. Agencies additionally need to employ multidisciplinary practices that drive towards higher orders of automation and the use of logical controls. To better maximize return on investment, agencies should be able to compare potential service offerings and use best-in-class contracts to acquire them.

Agencies should review their information technology portfolios to determine modernization plans for existing tools. They are encouraged to perform and leverage a full system and application rationalization, and those that have not begun this process are encouraged to start immediately. As part of this effort, agencies should consider whether virtualization, containerization, and other modern practices can be leveraged to increase efficiency in agency-owned data centers and vendor offerings. In accordance with the Federal Information Technology Acquisition Reform Act (FITARA), this process should be overseen by the Chief Information Officer (CIO) at the agency level to help identify potential opportunities for enterprise-wide improvement.

II. Security

In the 2017 Report to the President on Federal IT Modernization, the Administration outlines the future of Federal information technology as one in which agencies move further toward a risk-based approach to securing their systems that places appropriate emphasis on data-level protections and fully leverages modern virtualized technologies. This renewed focus must be driven by agency leadership, mission owners, IT practitioners, and governance bodies.

The evolution of the Federal Government’s cybersecurity policy and capabilities is essential to modernization. To implement a risk-based approach to cloud adoption, agencies should transition to security and protections at the data layer instead of the network and physical infrastructure layers, as well as improve the governance of systems. Additionally, it is critical that agencies have comprehensive visibility of their data, both on-premises and in the cloud, and perform continuous monitoring in order to detect malicious activity. As agencies approach their modernization efforts, they should apply these capabilities to their high-risk, high-value assets first in order to take advantage of all that cloud has to
offer.

The following programs are large elements of the current security strategy that must evolve with the changing technology landscape. However, with this update, agencies will need to think in terms of intended outcomes and capabilities, not merely programs, in approaching security holistically.

**Trusted Internet Connections**

In 2007, M-08-05 Implementation of Trusted Internet Connections (TIC) was released, with the purpose of standardizing the security of external network connections used by Federal agencies while reducing the number of those external network connections. The Trusted Internet Connections policy was established when agencies maintained the majority of their systems within their agency-owned and operated networks, and when networking was constrained by physical limitations. Since then, the technology landscape has changed dramatically with the proliferation of private-sector cloud offerings, the emergence of software-defined networks, and an increase in the mobile workforce. Improvements to security are now driven by standards and secured connections instead of limited physical connections.

In the current landscape, requiring all agency network traffic to flow through a limited number of Trusted Internet Connections is no longer feasible as a one-size-fits-all strategy. This design choice has hampered agencies’ ability to acquire new technologies including commercial cloud solutions, which use a distributed network model and use virtual, rather than physical, controls of data. In addition, these infrastructure designs have reduced agencies’ ability to take advantage of new paradigms such as the ability to create zero trust networks not bound by traditional firewalls.

As a result of these constraints, various agencies have worked with the Department of Homeland Security to establish agency-specific solutions to alleviate related performance degradation issues. The result of this work will be shared in a manner to reinforce alternative approaches to meeting Trusted Internet Connection objectives, including updating the Trusted Internet Connections Reference Architectures to demonstrate use cases where program objectives can be met without the requirement to route all traffic through a limited number of physical access points. In use cases where traffic is not required to be routed through a Trusted Internet Connection, agencies must implement DHS-designated controls required to ensure an appropriate baseline level of security across the Federal enterprise. Given the variety of platforms and implementations across the Federal enterprise, the Trusted Internet Connection Reference Architectures will also demonstrate how different use cases that do not require traffic to be routed through a Trusted Internet Connection can address the requirements for government-wide intrusion detection and prevention efforts, such as the EINSTEIN Program.4

**Continuous Data Protection and Awareness**

Migrating to a cloud-based environment changes the dynamic of network visibility and data protection that an agency might already be supporting. As data transits various networks and comes to rest in various locations, such as an end user’s device, Identity and Credential, and Access Management (ICAM) and encryption become increasingly important.

An agency is the custodian of its data on behalf of the public. As such, each agency should determine its own governance model for cloud-hosted data that aligns with their identity and credential management systems. Additionally, where a cloud solution is deployed by a vendor, a Service Level Agreement (SLA) should be in place that provides the agency with continuous awareness of the confidentiality, security, and availability of its data.
Furthermore, agencies should be made aware if their data resides on third-party information systems, provided with access to log data, and notified promptly if a cyber-incident or other adverse event occurs. Agencies should consider having an agreement with all providers, be they Federal or commercial, regarding access to and use of log data for their information security operations.

Agencies and their partners should regularly engage in reciprocal information sharing in an effort to combat malicious cyber behavior. Cybersecurity requires public-private collaboration, and as more Federal entities adopt commercial cloud solutions, customers and providers should work together to protect information. Furthermore, DHS’s Continuous Diagnostics and Mitigation (CDM) program must continue to evolve in order to equip agencies with the monitoring tools and capabilities they need to understand their cyber risk in the cloud.

**FedRAMP**

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that has proven the value of a standardized approach to security assessment, authorization, and continuous monitoring for large cloud services providers. Cloud service providers have shown their ability to meet Federal security requirements through standardized baselines and common criteria. With the growing marketplace of providers, agencies have been able to rapidly adapt from old, unsecured legacy technology to mission-enabling, secure, and cost-effective cloud-based systems.

Although the FedRAMP project management office has been able to drastically reduce the time to authorize a cloud service provider by working through the Joint Authorization Board, there is still work that can be done to improve the pace of authorizing new providers. In addition, the large number of agency-specific processes has made it complicated for agencies to issue an Authorization to Operate (ATO) for solutions, even when using existing authorized cloud service providers. In fact, despite the importance to cybersecurity risk management, agencies continue to cite major obstacles with their own policies and practices, which has transformed the ATO process from a risk-enabling practice to a labor-intensive exercise. Strategies for accelerating common ATO agreements and overall process improvements are in development and will be addressed in future guidance.

Leveraging cybersecurity expertise in the FedRAMP program will allow the Federal Government to continue to increase the efficiency and effectiveness of agency security practices in adopting cloud systems, while eliminating the burden on security professionals, providers, and agency leadership.

**III. Procurement**

In an effort to help Government move to the cloud, individual agencies, interagency working groups, and industry partners have provided a plethora of recommendations to Federal information technology and acquisition professionals. However, there has been a lack of consistent government-wide guidance or cross-agency information sharing on best practices. This has forced agencies to search across multiple sources to gain a basic understanding of the various types of cloud services sold in the commercial marketplace, the different offerings available on existing government-wide contracts, and the best way to evaluate which approach is best for a given requirement.

As a result of ubiquitous private sector use of cloud computing, agencies often purchase services through contracts that, while not specifically designed to purchase services or capabilities, involve placement of agency information into the cloud for processing or storage. This creates potential security concerns that require greater attention in order to ensure that the workforce has the tools necessary to reduce security risks and protect Government data.
To address these challenges, agencies will need to use a variety of approaches that leverage the Federal Government’s strengths in bulk purchasing power and shared knowledge of good acquisition principles. As part of the Cloud Smart multidisciplinary approach, they will also need to put security considerations at the forefront of any procurement efforts.

**Category Management**

The absence of any government-wide guidance or common standards and the limited collaboration across agencies has delayed the adoption of cloud within the Federal Government. This has also resulted in costly redundancies and inefficiencies for agencies that have procured cloud services.

The Federal Government will employ category management 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. Category management involves a structured approach focused on defining products and services that behave in a similar matter. It allows the Federal Government to buy smarter and more like a single enterprise, increases efficiency and effectiveness, and improves relationships with industry.

**Service Level Agreements**

A Service Level Agreement defines the level of performance expected from a service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved. In the Government acquisition context, the need for these agreements are incorporated via contract clauses and quality assurance provisions. In legacy technology environments, these agreements are a critical element of negotiation with suppliers. The term “Service Level Agreement” itself has become overloaded with multiple meanings depending on context and has resulted in increased uncertainty in how to achieve better outcomes for agencies. In order to ensure smarter cloud purchasing and usage across executive agencies, a two-track approach is needed.

First, a review and determination on contractual terms and conditions should be performed. Per the Federal Acquisition Regulations (FAR), contracts for procuring commercial items must include only those contract clauses required to implement provisions of law applicable to the acquisition of commercial items or determined to be consistent with customary commercial practice. Therefore, the Federal Government needs to ensure that any additions to customary commercial agreements focus on the goal of avoiding inconsistencies between commercial regulation and Federal law. This must be accomplished without unduly burdening industry or creating actual risks from changes to commercial practices.

Second, the President’s Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure stressed that heads of executive departments and agencies are accountable for managing the risk to their enterprises and that responsibility cannot be outsourced via Service Level Agreements. Many recommendations point to the potential benefits of clarifying roles and responsibilities, establishing clear performance metrics, and implementing remediation plans for non-compliance. An important element of acquiring cloud services is clarity in what services a cloud provider performs and at what level. Such governance, architecture, and operational clarity would help agencies ensure services are performed effectively, efficiently, and securely.

This two-track approach will decrease costs to Government and burdens on industry, enable faster procurement lead times, and reduce administrative costs for both Government and compliant commercial suppliers. Such an approach will increase standardization across Government usage of
cloud and mitigate the risks associated with siloed efforts at executive agencies.

**Security Requirements for Contracts**

It is incumbent on agencies to consider security implications while making cloud procurement and deployment decisions. To begin this shift in approach, the Office of the Federal Chief Information Officer will release an update to the previous High Value Asset (HVA) memorandum9 that builds on the previous initiative. Specifically, agencies need to ensure that contracts for High Value Assets, including those managed and operated in the cloud, include requirements to ensure visibility into the security of the asset. Additionally, agencies should include requirements for developers, manufacturers, and vendors to employ systems security and privacy engineering concepts. This will drive targeted integration of security and privacy design principles, secure coding techniques, and trusted computing methods.

**IV. Workforce**

The Federal information technology workforce is responsible for executing agency missions, delivering services to the public, and securing our nation’s critical systems and information. In the same way that agencies cannot outsource risk, neither can they outsource critical decision making to vendors. Agencies should instead infuse their own workforce with key skills to move the Cloud Smart strategy forward. Improving the Federal Government’s technology infrastructure to enhance the quality, security, and impact of services agencies deliver to taxpayers, requires maturity of the Federal workforce.

As agencies adopt and migrate to cloud platforms, the impact these migrations will have on the Federal workforce needs to be examined, along with identification of potential skill gaps. Agencies must forecast which new skills and programmatic approaches will be needed to address the gaps and skills evolution. For example, migration to cloud technologies may reduce needs for information technology hardware management but will likely increase the need for programming skills in the use of Infrastructure as Code. Agencies may also need to equip their acquisition staff with additional skills and knowledge to keep up with the ever-expanding list of technology options available to procure. Agencies’ cloud strategies and policies should generally include a workforce development and planning component that includes the following topics and activities.

**Identifying Skill Gaps for Current and Future Work Roles**

In order to successfully transition to cloud platforms, agencies will need to ensure that their workforce is knowledgeable enough to understand all of the considerations in planning a migration, as well as to support the cloud environment once deployed. Agency Chief Information Officers and Chief Human Capital Officers (CHCOs) should work collaboratively to conduct a skills gap analysis that is compliant with any statutes or regulations. At a minimum, the skills gap analysis should include an examination of the agency’s current IT workforce posture that is mapped to a projection of future skill and position requirements. Where appropriate, agencies are strongly encouraged to leverage industry projections to help predict future workforce skill and position requirements, especially for information technology roles. As with many new technology initiatives, agencies should expect to have an aggressive period in which staff are trained in the use of cloud technologies, as well as plan for ongoing training and experimentation in this very rapidly evolving field, where skills may become outdated in less than a year.
The Federal Cybersecurity Workforce Assessment Act of 2015 requires Federal agencies to implement the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework through a new coding structure and by identifying all Federal civilian positions performing information technology, cybersecurity, or other cybersecurity-related functions. While it is important for all agencies to participate in this process to help standardize the way in which the Federal Government assesses cybersecurity workforce gaps, this effort is not entirely inclusive of all information technology positions or skill sets. Therefore, agencies are encouraged to conduct a separate enterprise-wide IT skills gap analysis to ensure it is inclusive of all current and future information technology relevant skills and positions.

Reskilling and Retaining Current Federal Employees

Current employees may lack the skills or knowledge required to facilitate a cloud migration or to maintain the environment once migrated. It is important for the agency to conduct a skills gap analysis to identify both technical and non-technical skill and position gaps. Once the agency has identified those gaps, leadership will need to determine which skill and position gaps are the most significant and/or critically needed to support the agency’s mission.

In order to immediately address the most critical gaps, the agency will need to develop and implement reskilling strategies for current employees. Agency reskilling strategies should focus on training and professional development opportunities that allow current employees to acquire critically needed skill sets and certifications.

Reskilling initiatives should also include Senior Executives Service employees in order to provide them with a fundamental understanding of cloud computing. Additionally, acquisition of cloud computing services remains relatively new territory for acquisition professionals. Therefore, acquisition professionals such as Chief Acquisition Officers, Contracting Officers, and Project Managers will need to leverage current procurement resources and guidance. These resources should include those provided by the Office of Federal Procurement Policy and training opportunities such as those provided through the Federal Acquisition Institute and the TechFAR HUB.

Furthermore, consistent with guidance for specialized IT acquisition roles, agencies may benefit from reviewing their current IT acquisition workforce and program needs to determine if developing a new specialized team, or expanding the use of IT acquisition cadres, would lower cloud migration risk and improve overall outcomes. One possible model for training and development is the Office of Management and Budget’s Digital Information Technology Acquisition Professional (DITAP) program.

Lastly, agencies should consult with their Chief Human Capital Officers and Chief Learning Officers to determine the best approaches for training and redeployment options such as certification programs, creating merit promotion job opportunities, or rotational programs.

Recruiting and Hiring to Address Skill Gaps

The Bureau of Labor Statistics reports that cloud computing is a major factor in technology occupation growth, which is projected to expand 13% from 2016 to 2026. In addition to agencies reskilling current employees in order to address the most critical skill and position gaps, recruitment and hiring strategies should be considered. Key strategies include leveraging industry recruitment best practices, expanding the use of pay flexibilities, and removing bureaucratic barriers to hiring staff expeditiously. Agencies must build a pipeline to continuously feed cybersecurity talent into the Federal Government.
The market for technology professionals with cloud computing skill sets is extremely competitive. When possible, agencies should leverage techniques used by the private sector to attract and hire the best candidates to the Federal Government. In coordination with their Chief Human Capital Officer, agencies should execute proactive recruitment strategies such as:

- Attending industry conferences with career fairs;
- Holding national hiring events to strengthen awareness and outreach;
- Developing “most wanted” talent advertisements to showcase critical needs;
- Ensuring that job postings on places like USAJOBS properly reflect needed skills;
- Engaging candidates through social media platforms;
- Profiling and sharing current employee experiences;
- Leveraging merit promotion hiring procedures to retain, promote, or redeploy current Federal employees when appropriate; and
- Showcasing diversity and inclusion initiatives.

While the Government invests in efforts to recruit existing talent to the Federal workforce, it should also build a talent pipeline to expand the pool of qualified applicants. Through the Workforce Council and Chief Information Officer Council (CIOC) initiatives, the Government will continue to develop partnerships with community colleges, apprenticeship programs, and four-year institutions, in addition to leveraging partnerships that already exist. Expanded consideration of reskilling and upskilling solutions should be included in agency transition strategies.

**Employee Communication, Engagement, and Transition Strategies**

Prior to migrating to the cloud, agencies should execute communication plans that help employees understand the changes that will need to take place to implement the Cloud Smart strategy. For example, migration to the cloud may require decommissioning legacy systems that have been in use for many years. Employees may feel reluctant, especially if positions will be redefined, to learn to operate new systems in a cloud environment. Agencies can ease workforce concerns by clearly articulating how the current workforce will fit in once cloud adoption is complete. Socializing a technology roadmap to include systems that will be migrating to the cloud, either completely or partially, and an outline of the change management process to include reskilling opportunities is strongly recommended. Communicating and engaging with employees is key to successful adoption of new cloud solutions. Agencies should feel comfortable in leveraging vendors involved in cloud migration activities to provide or support training for current employees.

**Removing Bureaucratic Barriers to Hiring Talent Expeditiously**

The demand for technology professionals with cloud computing skills sets is at an all-time high. This means attracting, recruiting, and retaining the right individuals will take an executable human capital strategy with a streamlined hiring process. Agencies with aggressive hiring timelines and competitive offers leveraging pay and recruitment incentives will attract talent. It is imperative for agency leadership to identify and promptly address bureaucratic barriers that hinder agencies from hiring talent in an expeditious manner.
Agencies have broad authorities under Title 5 of the United States Code to hire top IT and cybersecurity talent, and to provide candidates with superior qualifications or who address critical skill gaps with pay flexibilities and incentives. Agencies are strongly encouraged to use available hiring authorities, recruitment, and student loan repayment incentives to hire professionals with highly sought-after cloud computing skills.

It is incumbent upon Federal agencies to ensure that their current and future workforce is prepared to support Federal cloud environments. Agency cloud strategies should enable leaders to develop and empower the information technology and cybersecurity workforce with the skills required to achieve cloud migration goals and support the latest technology that will improve critical citizen services.

1. 40 U.S.C. § 11319
2. https://itmodernization.cio.gov/
3. M-08-05 Implementation of Trusted Internet Connections (TIC)
5. https://www.dhs.gov/cdm
6. As established through Circular A-130, the Federal Information Processing Standards, and NIST Special Publications.
7. 48 C.F.R. § 12.301
8. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
9. M-17-09 Management of Federal High Value Assets
11. NIST Special Publication 800-181 – NICE Cybersecurity Workforce Framework
15. https://techfarhub.cio.gov/initiatives/ditap/