Skip to main content

**The site is secure.**
The **https://** ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely.

Menu

*Federal Cloud Computing Strategy*

- Cloud Smart
- CIO Council Actions

# From Cloud First to Cloud Smart

In the *Report to the President on Federal IT Modernization*, released publicly in 2017 in accordance with Executive Order 13800,[1] the Office of Management and Budget (OMB) pledged to update the Government's legacy Federal Cloud Computing Strategy ("Cloud First"). Fulfilling this promise, the Administration has developed a new strategy to accelerate agency adoption of cloud-based solutions: **Cloud Smart**.

Developed nearly a decade after its predecessor, Cloud Smart equips agencies with actionable information and recommendations gleaned from some of the country's most impactful public and private sector use cases.[2] Beyond Cloud First, which granted agencies broad authority to adopt cloud-based solutions, Cloud Smart offers practical implementation guidance for Government missions to fully actualize the promise and potential of cloud-based technologies while ensuring thoughtful execution that incorporates practical realities.

The new strategy is founded on three key pillars of successful cloud adoption: **security**, **procurement**, and **workforce**. Collectively, these elements embody the interdisciplinary approach to IT modernization that the Federal enterprise needs in order to provide improved return on its investments, enhanced security, and higher quality services to the American people.

## Key Actions

The Chief Information Officers Council (CIO Council) has developed a list of action items to execute the Cloud Smart strategy. These actions will constitute a work plan aimed at creating and updating programs, policies, and resources that the whole of Government will use to advance the Cloud Smart agenda.

Additionally, all Federal agencies will rationalize their application portfolios to drive Federal cloud adoption. The rationalization process will involve reducing an application portfolio by 1) assessing the need for and usage of applications; and 2) discarding obsolete, redundant, or overly resource-intensive applications. Decreased

application management responsibilities will free agencies to focus on improving service delivery by optimizing their remaining applications.

To support these rationalization efforts, the CIO Council will develop best practices and other resources. Furthermore, while the initial Cloud Smart work plan will be executed over an eighteen-month period, its actions will be refreshed continuously as needed to keep up with the changing cloud market and emerging technologies.

# I. Cloud at a Glance

## Redefining Cloud Computing

The term “cloud” is often used broadly in the Federal Government for any technology solution provided by an outside vendor. The National Institute of Standards and Technology (NIST) defined several cloud deployment models as progressive increases in management by vendors, from Infrastructure as a Service (IaaS) where vendors provide the infrastructure and hardware, to Platform as a Service (PaaS) where vendors provide a managed environment for a customer’s application, to Software as a Service (SaaS) where vendors provide a fully managed application and customers need only supply their data. In practice, many major vendor offerings no longer have such well-defined boundaries. Notwithstanding the term’s common usage, the term “cloud” is most accurately applied to those solutions that exhibit five essential characteristics of cloud computing, as defined by NIST: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service.[3]

These characteristics and the solutions that exhibit them are provider-agnostic – meaning anyone can develop and deploy a cloud solution, whether an outside vendor or a Federal agency. Industry has moved to a more finely differentiated set of capabilities offered at different system layers, making possible nearly any combination of various components managed by either a vendor, a Government agency, or a mix of both. Industries that are leading in technology innovation have also demonstrated that hybrid and multi-cloud environments can be effective and efficient for managing workloads. As a result, the Cloud Smart Strategy encourages agencies to think of cloud as an array of solutions that offer many capabilities and management options to enhance mission and service delivery.

Furthermore, Cloud Smart operates on the principle that agencies should be equipped to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations. Computing and technology decisions should also consider customer impact balanced against cost and cybersecurity risk management criteria. Additionally, agencies need to weigh the long-term inefficiencies of migrating applications as-is into cloud environments against the immediate financial costs of modernizing in advance or replacing them altogether.

Cloud adoption strategies that successfully meet the intent of Cloud Smart should not be developed around the question of who owns which resources or what anticipated cost savings exist. Instead, agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources.

## Modernization and Maturity

To realize the full benefit of cloud technology, agencies must cultivate an organizational mindset of constant improvement and learning. Modernization is not a commitment that is sustained solely by 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. Critical to fostering this mindset of constant improvement is agency leadership’s prioritization of the training and education of their staff, detailed and comprehensive migration planning, and a focus on balancing solution sustainability with the incorporation of new capabilities into agency operating

environments. To that end, agencies will need to iteratively improve policies, technical guidance, and business requirements to match changing needs, drive positive outcomes, and prevent their IT portfolio from becoming obsolete.

Agencies should conduct regular evaluations of customer experience and user needs to ensure that their solutions successfully foster efficiency, accessibility, and privacy.[4] Additionally, agencies should regularly rationalize and update their applications, migrating as needed, to reduce the risk of large-scale failure, better allocate their resources, and provide staff with adequate time to become familiar with contemporary product management techniques. Agencies must also track their growth in areas where decisions about technology intersect other disciplines. Namely, serious consideration and investment should be dedicated to the three key pillars of successful cloud adoption: **security, procurement,** and **workforce.**

Given the distributed nature of cloud and the growing number of discrete capabilities and deployment models available to choose from, agencies might consider moving or adding security and privacy controls to the data layer itself, rather than just where they have historically resided at the network perimeter. By doing so, agencies can improve their overall security and privacy posture, empowering them to fully embrace cloud technologies while granting them peace of mind that the confidentiality and integrity of their data are intact.

To realize not only the security benefits of cloud infrastructure, but also its benefits related to scalability and speed-to-market, agencies should utilize mature agile development practices, including DevSecOps. The use of automated and assistive technologies such as artificial intelligence and machine learning can help agencies to further improve security. Agencies should also review their IT portfolios regularly to determine modernization plans for existing tools and compare potential service offerings designated as Best In Class (BIC) solutions for maximized return on investment.

Furthermore, providing staff with training and other educational resources is essential to fostering maturity in the areas of privacy, security, and procurement. Agency IT staff should become familiar with lean product management, agile development, continuous delivery, and automated infrastructure at the team and program level as part of any modernization plan. Additionally, non-IT staff supporting privacy, security, and procurement should receive training in the multiple core disciplines outlined above. Sustained progress in these areas of staff training is foundational to the successful implementation of new cloud efforts.

Consistent with the requirements of the Federal Information Technology Acquisition Reform Act,[5] the agency Chief Information Officer (CIO) should oversee modernization processes to help find opportunities for enterprise-wide improvement. Additional involvement of the Chief Financial Officer can help properly budget for planning, evaluation, and technology adoption. CIOs should also incorporate feedback from business units and end users affected by modernization projects to minimize disruption to mission delivery.

# II. Security

Agencies should take a risk-based approach to securing cloud environments. As recommended by the *Report to the President on Federal IT Modernization*, agencies should emphasize “data-level protections and fully leverage modern virtualized technologies.”[6] This requires that agencies place an emphasis on protections at the data layer in addition to the network and physical infrastructure layers, transitioning to a multi-layer defense strategy, otherwise known as defense-in-depth.

Critical to the success of this security strategy in the context of Cloud Smart is the assurance of confidentiality, integrity, and availability of Federal information as it traverses networks and rests within systems, regardless of whether those environments are managed locally, off-premises, by a Government entity, or by a contractor. Additionally, it is essential that agencies perform continuous monitoring to detect malicious activity and dedicate effort to improving systems governance.

Successfully managing cloud adoption risks requires collaboration between agency leadership, mission owners, technology practitioners, and governance bodies. Coordination between information security and privacy programs is necessary to ensure compliance with applicable privacy requirements and for the successful identification and management of risks to individuals when processing personally identifiable information (PII).[7] Senior Agency Officials for Privacy (SAOPs)[8] are responsible for managing the risk that may result from the creation, collection, use, and retention of PII, and have an important role to play when making decisions about the adoption of technology and processes that concern or impact the management of PII.

**Cloud Smart** encourages agencies to approach security and privacy in terms of intended outcomes and capabilities. The following programs are major elements of the Federal security strategy that must evolve alongside technological progress to allow agencies to take such a holistic and outcome-driven approach.

# Trusted Internet Connections

Released in 2007, OMB Memorandum M-08-05[9] established new requirements for Federal agencies with the intent to reduce the Federal-wide number of external network connections while standardizing their security. Since the policy's release, agency network traffic in compliance with OMB requirements has flown exclusively through a limited number of external connections, known as Trusted Internet Connections (TICs). While this initial architectural concept served an important purpose at its inception, at a time when networking was constrained by physical limitations and agency approaches to network security were not standardized and highly fragmented, the technology landscape has evolved to provide agencies with more tools, technologies, and approaches to secure their data, leaving the once-useful TIC construct now relatively inflexible and incompatible with many agencies' requirements. With the proliferation of private-sector cloud offerings, the emergence of software-defined networks, and an increasingly mobile workforce, the TIC model must compete with newer, more flexible solutions that provide equal or greater security, or it must evolve as well.

Electing the latter option, the Department of Homeland Security (DHS) is working with various agencies to pilot agency-specific approaches that meet the objectives and intent of M-08-05 while minimizing technical constraints posed by the policy's one-size-fits-all TIC model. These newer, less rigid approaches will be incorporated into updated TIC Reference Architectures to highlight use cases wherein security objectives can be met without routing all traffic through a prescribed set of physical access points. The TIC Reference Architectures will also demonstrate how different use cases that do not require traffic to be routed through a TIC can address the requirements for government-wide intrusion detection and prevention efforts, such as the EINSTEIN Program while also incorporating DHS-designated controls, which have been designed to ensure a baseline level of security across the Federal enterprise.[10]

By taking these actions to expand the options available to agencies to secure their networks and data, the collective ability of the Federal Government to take advantage of new paradigms, such as zero trust networks, is heightened, as its effectiveness in managing risk.

# Continuous Data Protection and Awareness

Given the ease of flow of federally-owned data from internal networks to external, end-user devices, encryption and modern Identity, Credential, and Access Management (ICAM) implementation is essential. Encryption and ICAM implementation is particularly relevant in the context of cloud-based environments, namely in those instances where an agency is partnering with an external service provider to manage network visibility and data protection.

To ensure continuity of information security during and after the migration process, it is incumbent upon agencies to thoroughly assess their operational, policy, and business requirements and advocate for themselves when brokering new arrangements with cloud service providers. Regardless of provider type – commercial or Federal – agencies should consider having agreements in place with all providers regarding access to, and use of,

log data given its importance in effectively conducting information security operations. Moreover, as each agency is the custodian of its information on behalf of the public, each agency is responsible for determining its own governance model for cloud-hosted data that aligns with its identity and credential management systems. To that end, 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, integrity, and availability of its information.

Furthermore, agencies should be made aware if their information will reside on a third-party information system prior to signing any service agreement; agencies should be provided continuous access to log data; and must be notified promptly if a cybersecurity incident, breach, [11] or other adverse event occurs or is suspected to have occurred that involves any information or information systems covered by a service agreement with a cloud service provider.

To further enable continuous data protection and awareness, agencies and their partners should regularly engage in reciprocal information sharing. Cybersecurity requires public-private collaboration, and as more Federal entities adopt commercial cloud solutions, customers and providers should work together to protect information. Recognizing the criticality of tools and analytical capabilities that scale across multi-cloud environments in the facilitation of continuous visibility and information sharing, DHS's Continuous Diagnostics and Mitigation (CDM) Program[12] also continues to evolve so that agencies are equipped with the monitoring capabilities they need to understand their cyber risk in the cloud.

# FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized government-wide approach to security assessment, authorization, and continuous monitoring of cloud services. Offering cloud service providers the opportunity to demonstrate their ability to meet Federal security requirements through standardized baselines has allowed for a flourishing marketplace of vetted providers to develop. It has also allowed agencies to adapt from arcane legacy technology to mission-centric and cost-effective cloud-based systems in a more rapid, consistent, and secure manner.

Although the FedRAMP program management office has drastically reduced the amount of time it takes to authorize a cloud service provider, there is still work to be done to address the underlying issues that contribute to the relatively slow pace of assessment. For example, a lack of reciprocity across agencies when adopting FedRAMP authorizations has led to significant duplication of effort when assessing security for product deployment. In addition, a 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 reiterated importance of enterprise risk management,[13] agencies continue to cite major obstacles with their own policies and practices.

To tackle these challenges, several initiatives aimed at overall process evolution as well as strategies for accelerating common ATO agreements are under development. These efforts intend to drive better and more automated control inheritance and monitoring, a prioritized approach to control implementation, and more normalized control use across the Federal enterprise. Advancements to cloud ATO development will be used to inform overall ATO reform, which will involve the revision of NIST special publications. This will also reestablish FedRAMP's role in the risk assessment process as a verification check for agencies as they make informed decisions about the cloud solutions that they deploy, rather than a panacea for all matters related to the risk associated with any implementation of a cloud solution. OMB and GSA will continue to promote alignment and reuse of ATO determinations and closely examine agency-identified obstacles in that effort.

Finally, enhancing the skillsets of the Federal workforce around cloud security 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 reducing the burden on security professionals, providers, and agency leadership. Assembling a cadre of professionals and providing direct engagement with all aspects of the security

authorization process will build a common and comprehensive understanding of cloud security and enable more trust when sharing ATOs. Agencies are also encouraged to take a multidisciplinary approach to hiring and training their workforce, as well as provide community spaces where digital services experts, information security professionals, procurement specialists, and others with a mutual interest in effective, secure cloud adoption can collaborate on current challenges and opportunities in the cloud computing space.

# III. Procurement

Industry partners, interagency working groups, and individual agencies have provided the Federal IT and acquisition communities with a wide selection of recommended actions to accelerate the adoption of cloud solutions. Some of these recommendations have been translated into Federal-wide guidance, but there remains a lack of consistency across agency implementations and information sharing on best practices. In the absence of comprehensive guidance, agencies must 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 marketed as a cloud-based service or capability, involve placement of agency information into cloud-based systems for processing or storage. This trend creates potential security and privacy concerns and warrants that agencies pay greater attention to professional services contracts, where the storage of Federal information on non-Government information systems may be implied.

To address these challenges, agencies will need to use a variety of approaches that leverage the strength of Federal Government's bulk purchasing power, the shared knowledge of good acquisition principles, as well as relevant risk management practices. As part of the Cloud Smart multidisciplinary approach, agencies will also need to place security and privacy considerations at the forefront of any procurement effort, and to avoid vendor lock-in, they should evaluate the business process dependencies of any new solution. They should also update their business continuity and disaster recovery plans to include contingencies involving the sudden interruption or termination of service. Detailed below are additional considerations for Federal procurement professionals navigating the IT space and IT professionals seeking guidance on common practices to ensure the cost-effective, safeguarded procurement of cloud-based solutions.

## Category Management

Category management describes the strategic business practice that the Federal Government is implementing to buy smarter and more like a single enterprise. Specifically, government-wide category management aims to: 1) deliver more savings, value, and efficiency for Federal agencies; 2) eliminate unnecessary contract redundancies; and 3) meet the Government's small business goals.

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. OMB has published a memorandum[14] that outlines guidance on the implementation of category management principles and use of common contract solutions.

## Service Level Agreements

A Service Level Agreement (SLA) between a customer and a service provider 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. While not standardized in the Federal Acquisition

Regulation (FAR),[15] SLAs are incorporated through contract clauses and quality assurance contractual provisions. In legacy technology environments, these agreements represent a critical element of negotiation with suppliers. Unfortunately, the term "Service Level Agreement" itself has become overloaded with multiple meanings depending on context, which has resulted in increased uncertainty around the best approach to achieve better outcomes for agencies. Cloud Smart offers a two-track approach to smarter cloud purchasing and usage across Federal agencies through improvements to SLA use, as outlined below.

First, it is important to note that candidates for inclusion as standard clauses that apply to commercial items in the FAR – including new SLAs – must generally meet at least one of the following criteria: (1) the clause is required to implement a provision of law applicable to the acquisition of commercial items; or (2) the clause is generally consistent with customary commercial practice. Keeping these stipulations in mind, the first track of activities to support the effective use of SLAs involve the government-wide review and selection of contractual terms and conditions specific to cloud-based commercial offerings that are good candidates for standardized use across agencies. Standardizing cloud contract SLAs will provide more effective, efficient, and secure cloud procurement outcomes for agencies, while also enabling enhanced management of risk across the Federal enterprise through greater consistency and transparency in negotiations with commercial suppliers.

Second, heads of executive agencies are accountable for managing the risk to their enterprises, and that responsibility remains with the agency head even with respect to contractor-operated systems. An important element of acquiring cloud services is clarity in what services a cloud provider performs and at what level. Therefore, to facilitate effective risk management by way of their relationships with commercial cloud service providers, agencies should granularly articulate roles and responsibilities, establish clear performance metrics, and implement remediation plans for non-compliance. Such governance, architecture, and operational clarity would help ensure that services are performed as intended, and, when paired with the right SLA language, would offer agencies a way to mitigate risk while optimizing the performance and efficiency of their newly procured cloud-based solution.

## Security Requirements for Contracts

It is essential that agencies consider and manage security and privacy risk to information and mission services when making cloud procurement and deployment decisions. Incorporating this approach as part of the acquisitions process and system development lifecycle, the Federal CIO has published an updated High Value Asset (HVA) memorandum[16] that builds on the previous initiative and adds considerations for managing risk across hybrid environments. Agencies must now ensure that contracts impacting their HVAs, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset. The guidance enables agencies to proactively assess the security and privacy posture of their assets and seeks to increase HVA trustworthiness by requiring developers, manufacturers, and vendors to employ best practices for designing, deploying, and securing systems. This will drive a targeted integration of security and privacy design principles, secure coding techniques, and trusted computing methods.

# IV. Workforce

The Federal IT workforce plays an integral role in the execution of agency missions, delivery of services to the public, and provision of security to the nation's essential systems and information. In the same way that agencies cannot outsource risk to commercial suppliers, neither can they outsource decision-making. Agencies' immediate and sustained investment in the Federal workforce is critical to the enhanced quality, security, and impact of services delivered to taxpayers. Without it, improvements to the Federal Government's technology infrastructure, and the successful proliferation of the Cloud Smart strategy will not be fully realized.

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 skills 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.

Agencies should not restrict themselves to a single model for workforce transformation. Strategies might include development programs for emerging talent or future leaders; apprenticeship programs; initiatives to convert non-IT personnel where aptitudes align; or exchanges of qualified personnel through public-private partnerships or interagency detail opportunities. Generally, agencies' cloud strategies and policies should also include a workforce development and planning component that tailors a transformation and training approach to that agency. Additionally, in the event that an impact to the existing workforce has been identified, this approach should include a cross-walk of new skills and occupational categories with legacy occupational categories to foster clarity and ease of transition.

## Identifying Skill Gaps for Current and Future Work Roles

Successful adoption of cloud solutions requires a workforce that understands how to manage the complexities of a migration as well as how to support a cloud environment once fully deployed. Agency CIOs, Chief Human Capital Officers (CHCOs), and SAOPs should collaboratively conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements. Agencies are strongly encouraged to leverage industry projections to help predict future workforce skill and position requirements, especially for IT roles.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, whose use by Federal agencies is mandated in the Federal Cybersecurity Workforce Assessment Act of 2015[17], recommends an approach for identifying all Federal civilian positions performing IT or cybersecurity-related functions.[18] While Federal agencies should continue to comply with the 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.

## 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. Therefore, agencies must conduct their skills gap analysis to identify both technical and non-technical skill and position gaps so that leadership may determine which deficiencies are the most significant and/or represent a critical mission need.

Agencies should address the most pressing deficits found by a workforce gap analysis by developing employee reskilling strategies that focus on training and professional development opportunities, such as OMB's Digital Information Technology Acquisition Professional (DITAP) program.[19] A complete reskilling strategy will account for technical as well as non-technical needs. Given that cloud computing is relatively new territory for acquisition professionals, such as Chief Acquisition Officers, Contracting Officers, and Project Managers, should take advantage of existing guidance from resources such as the OMB, the Federal Acquisition Institute,[20] and the TechFAR HUB.[21] Consistent with guidance for IT acquisition roles, agencies may also benefit from developing a specialized team or expanding the use of IT acquisition cadres.[22]

Lastly, CHCOs and Chief Learning Officers should help determine optimal training and redeployment options (e.g., certification and rotational programs) to utilize reskilled employees. As with many new technology initiatives, agencies should expect an aggressive initial training period and should also plan for ongoing education and experimentation in this rapidly evolving field. Providing valuable employees access to continuing education resources and opportunities to apply their knowledge will both inform new cloud initiatives and promote job satisfaction.

Above all else, the success of initiatives like these is dependent on the support of champions in executive leadership who broadly vocalize their backing of the effort and who remove roadblocks that discourage or prevent employees from pursuing reskilling or certification opportunities. While finding the right champion presents its own challenges, the ability of this person to amplify the reach and results of the agency's initiative is invaluable.

# Recruiting and Hiring to Address Skill Gaps

The U.S. Department of Labor's 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.[23] In addition to reskilling current employees to address the most critical skill and position gaps, agencies should continuously evaluate and update their recruitment and hiring strategies. 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 and IT 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 Officers, agencies should execute proactive recruitment and retention 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;
- Offering incentives to employees for relevant professional development;
- Supporting engagement of Federal employees in appropriate industry forums to increase visibility and access;
- Leveraging merit promotion hiring procedures to retain, promote, or redeploy current Federal employees when appropriate;
- Leveraging hiring and retention authorities approved by the Office of Personnel Management, such as incentive pay and awards;
- Leveraging Scholarship for Service and other academic partnership to build a pipeline for graduates into the Federal Government; 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, Federal Privacy Council, and the Chief Information Officer Council 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 as well.

## Employee Communication, Engagement, and Transition Strategies

As agencies implement the Cloud Smart strategy, they should execute communication plans that help employees understand the changes that will occur. 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 align 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. Agencies should also feel comfortable 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 that attracting, recruiting, and retaining the right individuals will take an executable human capital strategy with a streamlined hiring process and non-traditional incentives. 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 incentives, and student loan repayment benefits 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 and commensurate workforce investments should enable leaders to develop and empower the IT and cybersecurity workforce with the skills required to achieve cloud migration goals and support the latest technology that will improve delivery of critical citizen services.

# V. Conclusion

To be Cloud Smart, agencies must consider how to use their current resources to maximize value: reskilling and retraining staff, enhancing security postures, and using best practices and shared knowledge in acquisitions. Cloud Smart is about equipping agencies with the tools and knowledge they need to make these decisions for themselves, rather than a one-size-fits-all approach.

By leveraging modern technologies and practices, agencies will be able to harness new capabilities and expand existing abilities to enable their mission and deliver services to the public faster. To make this shift, instead of “buy before build”, agencies will need to move to “solve before buy,” addressing their service needs, fundamental requirements, and gaps in processes and skillsets before starting on a new procurement. By rationalizing their application portfolios regularly, agencies can continue to make modernization progress while targets move with the ever-changing technology landscape.

Since the release of the original draft of this strategy, OMB has worked with its partners – both Government agencies and in the private sector - to update policy guidance and create new resources for aiding cloud adoption. Yet there will always be more work to be done, as technology does not have a finish line. Embracing change as a core business principle is critical to delivering the best return on investment to the American people.

Sincerely,

Suzette Kent

U.S. Federal Chief Information Officer

---

1. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* ↩
2. *Report to the President on Federal IT Modernization* ↩
3. NIST. "The NIST Definition of Cloud Computing." Special Publication 800-145 ↩
4. See Circular A-11, Section 280 for a discussion of customer experience requirements for agencies. ↩
5. 40 U.S.C. § 11319. ↩
6. https://itmodernization.cio.gov/ ↩
7. As defined in Circular A-130, the term "personally identifiable information" means […]. ↩
8. M-16-24, Role and Designation of Senior Agency Officials for Privacy ↩
9. M-08-05 Implementation of Trusted Internet Connections (TIC) ↩
10. https://www.dhs.gov/einstein ↩
11. As defined in OMB M-17-12, a breach is defined as "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." ↩
12. https://www.dhs.gov/cdm ↩
13. As established through Circular A-130, the Federal Information Processing Standards, and NIST Special Publications. ↩
14. M-19-13, Category Management: Making Smarter Use of Common Contract Solutions and Practices ↩
15. 48 C.F.R. § 12.301 ↩
16. M-19-03 Enhancing the High Value Asset Program ↩
17. https://www.congress.gov/bill/114th-congress/house-bill/2029/text ↩
18. NIST Special Publication 800-181 – NICE Cybersecurity Workforce Framework ↩
19. https://techfarhub.cio.gov/initiatives/ditap/ ↩
20. https://www.fai.gov/ ↩
21. https://techfarhub.cio.gov/ ↩

22. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/procurement/memo/guidance-for-specialized-acquisition-cadres.pdf ↩

23. Bureau of Labor Statistics – *Occupational Outlook Handbook: Computer and Information Technology Occupations*, as of April 2018 - https://www.bls.gov/ooh/computer-and-information-technology/home.htm ↩


**Office of Management and Budget**

**Office of the Federal Chief Information Officer**

*policy.cio.gov*

*ofcio@omb.eop.gov*