Department of Defense

Chief Information Officer

Cloud Computing Strategy

July 2012

FOREWORD

The DoD Cloud Computing Strategy has evolved to identify the most effective ways for the Department to capitalize on opportunities and take advantage of cloud computing benefits that accelerate IT delivery, efficiency, and innovation as an Enterprise. Prior drafts were informally coordinated and comments from across the Department were used to broaden the scope and depth of the current document; significant modifications and additions have been incorporated. In addition, DoD CIO and Defense Information Systems Agency (DISA) led a DoD Capability Assurance and Alignment Process (CAAP) Working Group to refine the approach and clarify required capabilities.

The DoD Cloud Computing Strategy has been expanded to address use of commercial cloud services in the Department's multi-provider enterprise cloud environment. Adoption and implementation of commercially provided cloud services are being rapidly accelerated with the maturing of the Federal Cloud Computing Initiative, the Federal Risk and Authorization Management Program (FedRAMP), and release of the 2012 National Defense Authorization Act.

I am pleased to provide this strategy to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud services. We will continuously seek to refine and mature the cloud computing approach and maintain open communications with all levels of the Department, other Federal Agencies and our Industry partners. Active participation and commitment of all DoD Components is critical to ensure consistency, optimize benefits and achieve the goal of this strategy.

Teresa M. Takai
DoD Chief Information Officer

This page intentionally left blank

EXECUTIVE SUMMARY

In the current political, economic, and technological landscape, information technology (IT) is expected to provide extensive and ever-increasing capabilities while consuming fewer resources. With the increase of both state-sponsored and independent cyber threats, the Department of Defense (DoD) is recognizing the growing importance of leading a strong and secure presence in cyberspace. Concurrently, global financial events are driving a need for continued budgetary constraints and stricter financial oversight. As a result, the Department must transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security.

The Department has begun this transformation by establishing a set of initiatives that are aimed at achieving improved mission effectiveness and cybersecurity in a reengineered information infrastructure. The result of this new effort will be the Joint Information Environment, or JIE. The Joint Information Environment is a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.

The DoD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE goals. The DoD Cloud Computing Strategy introduces an approach to move the Department from the current state of a duplicative, cumbersome, and costly set of application silos to an end state which is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. The DoD Chief Information Officer (CIO) is committed to accelerating the adoption of cloud computing within the Department and to providing a secure, resilient Enterprise Cloud Environment through an alignment with Department-wide IT efficiency initiatives, federal data center consolidation and cloud computing efforts. Detailed cloud computing implementation planning has been ongoing and informs the JIE projected plan of actions and milestones in Capabilities Engineering, Operation and Governance efforts.

DoD Cloud Computing Goal

Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device.

Increased mission effectiveness and operational efficiencies are key benefits that can be achieved with cloud computing. Cloud computing will enable the Department to consolidate and share commodity IT functions resulting in a more efficient use of resources. Cloud services can enhance Warfighter mobility through device and location independence while providing on-demand secure global access to mission

data and enterprise services. Cloud platforms and services can provide increased opportunity for rapid application development and reuse of applications acquired by other organizations.

The Department has specific cloud computing challenges that require careful adoption considerations, especially in areas of cybersecurity, continuity of operations, information assurance (IA), cybersecurity, and resilience. Additional challenges include service acquisition and funding sustainment, data migration and management, and overcoming network dependence at the tactical edge (disconnected, intermittent and low-bandwidth (DIL) users).

To help meet these challenges, the Department is leveraging the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP will establish a standard approach to assess and authorize cloud computing services, and define requirements for the continuous auditing and monitoring of cloud computing providers. In addition, DoD CIO is currently updating the Department's Information Assurance (IA) policies and instructions, aligning IA controls and processes with those used across the Federal Government. The Department is taking a cautious approach as it works to fully understand the challenges and establish the appropriate risk mitigations.

The DoD CIO is accelerating and synchronizing efforts that create enterprise-wide capabilities and services while eliminating the unnecessary duplication of capabilities. Currently, the Components are consolidating their data centers and network infrastructure. By designating a few data centers as "Core" Components can build in cloud infrastructure that begins the process of creating a DoD Enterprise Cloud Environment. This process will include network re-design and consolidation, policy and process changes, and the adoption of enterprise standards that enable interoperability across networks and between data centers. The DoD Enterprise Cloud Environment will include separate implementations and data exchanges on Non-secure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet), and Top Secret Sensitive Compartmentalized Information (TS SCI) security domains. This environment will be closely aligned with Intelligence Community- led initiatives, and support information sharing with DoD traditional and non-traditional partners on Joint Worldwide Intelligence Communications System (JWICS), and other networks.

In addition to enterprise cloud services provided Department-wide, Components will be encouraged to use or provide cloud services offered by other Components, other entities in the Federal Government, mission partners and commercial vendors that meet their specific mission requirements. All cloud services must comply with Department IA, cybersecurity, continuity, and other policies. The Department will leverage commercially offered cloud services that offer the same or a greater level of protection necessary for DoD mission and information assets. New guidance is being developed that will establish an Enterprise Cloud Service Broker to manage the use, performance, and synchronized delivery of cloud service offerings within the

Department, from other Federal, and commercial providers. The Broker will make it easier, safer, and more productive for DoD consumers to discover, access, and integrate cloud services to support their mission.

The Department has identified four concurrent steps that enable a phased implementation of the DoD Enterprise Cloud Environment:

Step 1: Foster Adoption of Cloud Computing

- Establish a joint governance structure to drive the transition to the DoD Enterprise Cloud Environment
- Adopt an Enterprise First approach that will accomplish a cultural shift to facilitate the adoption and evolution of cloud computing
- Reform DoD IT financial, acquisition, and contracting policy and practices that will improve agility and reduce costs
- Implement a cloud computing outreach and awareness campaign to gather input from the major stakeholders, expand the base of consumers and providers, and increase visibility of available cloud services throughout the Federal Government

Step 2: Optimize Data center Consolidation

- Consolidate and virtualize legacy applications and data

Step 3: Establish the DoD Enterprise Cloud Infrastructure

- Incorporate core cloud infrastructure into data center consolidation
- Optimize the delivery of multi-provider cloud services through a Cloud Service Broker
- Drive continuous service innovation using Agile, a product-focused, iterative development model
- Drive secure information sharing by exploiting cloud innovation

Step 4: Deliver Cloud Services

- Continue to deliver DoD Enterprise cloud services
- Leverage externally provided cloud services, i.e., commercial services, to expand cloud offerings beyond those offered within the Department

The DoD CIO will establish a joint enterprise cloud computing governance structure to drive the policy and process changes necessary to transition to the DoD Enterprise Cloud Environment and oversee the implementation of the DoD Enterprise Cloud Strategy. To achieve the cloud computing goal, all barriers to consolidation and transition must be addressed without major delay. DoD CIO will be the final decision authority and will provide oversight for Component execution of data center consolidation and cloud services, exercising appropriate governance to ensure an efficient orchestration of change.

Table of Contents

Introduction

As business and mission dependency on Information Technology (IT) grew within the DoD, duplicative, costly and complex IT infrastructures were built by Components to execute their missions and run their businesses. The development, operation, and management of these resources are largely inefficient, costing time and money that could be applied directly towards achieving strategic initiatives. According to a Defense Science Board analysis of 32 major automated information system acquisitions, the average time to deliver an initial DoD program capability is 91 months once funding is approved. This is two to three times the average industry IT refresh cycle time, making it difficult to keep pace with user needs and technology evolution. Continued technology maturation has enabled commoditization of certain IT functions (email, server hosting, collaboration, etc.), and improved network performance now allows IT organizations to specialize in offering these commoditized IT functions as services on the network.

The Department must take advantage of the commoditized IT functions and transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security. The Department has begun this transformation by establishing a set of initiatives that are aimed at achieving improved mission effectiveness and cybersecurity in a reengineered information infrastructure. The result of this new effort will be the Joint Information Environment, or JIE. The JIE is a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.

The DoD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE goals. The DoD CIO is committed to accelerating and synchronizing efforts to eliminate unnecessary duplication of capabilities with Enterprise-wide services, while establishing Enterprise security mechanisms to ensure secure connection and access control across mission partner and network boundaries. The DoD Enterprise Cloud Environment will facilitate consolidating and optimizing the Department's IT infrastructure, including data centers and network operations, and standardizing IT platforms that ensure a secure cyber environment and leverage Agile development. The Department will also adopt commercial cloud computing solutions to the greatest extent possible in support of the Department's mission. Detailed Cloud Computing implementation planning has been ongoing and informs the JIE projected plan of actions and milestones in Capabilities Engineering, Operation and Governance efforts.

DoD Cloud Computing Goal

Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device.

The Federal Cloud Computing Strategy (See Appendix B,(Reference A)) characterizes cloud computing as a:

> *"…profound economic and technical shift (with) great potential to reduce the cost of federal Information Technology (IT) systems while … improving IT capabilities and stimulating innovation in IT solutions."*

The DoD Cloud Computing Strategy lays the groundwork, consistent with the Federal Cloud Computing Strategy, for accelerating cloud adoption in the Department. It is intended to foster a substantive discussion as the Department transitions to its Enterprise Cloud Environment.

Cloud Computing Defined

The National Institute of Standards and Technology (NIST) defines cloud computing as:

> *"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

The details of the NIST cloud computing definitions provide a simple and unambiguous taxonomy of three service models available to cloud consumers that are the core of cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Detailed definitions of these three models appear in Appendix C, along with other terms typically associated with cloud computing, such as delivery models and characteristics.

While the traditional IT delivery model is focused on the development, maintenance and operation of computing hardware and software, the cloud computing model focuses on providing IT as a service. Under the cloud computing model, there are service providers and service consumers. Service providers specialize in performing specific tasks or functions for service consumers. The service providers and service consumers interact with one another over an Internet Protocol (IP)-based network.

Federal and DoD Mandates Driving Cloud Computing Adoption

The Federal Government intends to accelerate the pace at which it will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new IT investments. In alignment with Federal and Department-wide IT efficiency mandates, the DoD is committed to cloud computing, and to providing a secure, resilient Enterprise Cloud Environment. Specific mandates include:

- **2012 National Defense Authorization Act (NDAA) (Public Law 112-81):** The fiscal 2012 NDAA (See Appendix B,(Reference B)) mandates that DoD CIO submit a Performance Plan that includes a strategy to address "migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security" and "utilization of private sector managed security services for data centers and cloud computing services."

- **Secretary of Defense (SecDef) Efficiencies Initiative:** The SecDef announced a DoD-wide efficiencies initiative (See Appendix B,(Reference C)) to move America's defense institutions toward a "more efficient, effective, and cost-conscious way of doing business." This initiative directed the consolidation of IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs to improve DoD's ability to execute its missions while defending its networks against growing cyber threats.

- **Office of Management and Budget (OMB)-directed Federal Data center Consolidation Initiative (FDCCI):** The FDCCI (See Appendix B,(Reference D)) directed a reduction in data centers to be achieved primarily through the use of virtualization techniques and leveraging cloud computing.

- **Federal CIO 25 Point Implementation Plan to Reform Federal Information Technology Management:** The 25 point plan (See Appendix B,(Reference E)) specifies that "Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth by implementing a Cloud First policy for services, and increasing the use of available cloud and shared services."

- **Federal Risk and Authorization Management Program (FedRAMP):** FedRAMP (See Appendix B,(Reference F)) provides joint "provisional" authorizations and continuous security monitoring services applicable to "Executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources."

- **DoD IT Enterprise Strategy and Roadmap (ITESR)**: The ITESR (See Appendix B,(Reference G)) presents the DoD CIO's plan for achieving the goals of the SecDef's Efficiency Initiative and the mandates of OMB's FDCCI and 25 Point Implementation Plan.

Benefits DoD Can Derive From Cloud Computing

Table 2 of the Federal Cloud Computing Strategy (See Appendix B,(Reference A)) summarized three areas of cloud computing, reproduced in Table 1, below.

Table 1: Cloud benefits: Efficiency, Agility, Innovation

Efficiency	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data center Consolidation initiative) • Improved productivity in application development, application management, network, and end-user devices	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult to manage systems
Agility	
Cloud Benefits	**Current Environment**
• Purchase "as-a-Service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
Innovation	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-averse culture

Achieving DoD IT Objectives Through Cloud Computing

The desired outcomes of DoD's adoption and use of cloud computing will include reduced costs and increased IT service delivery efficiencies, increased mission effectiveness, and enhanced cybersecurity. These results, listed below, align with the benefits identified by the Federal Cloud Computing Strategy: Efficiency, Agility, and Innovation.

- **Reduced Costs/Increased Operational Efficiencies**
    - Consolidating systems, which reduces the physical and energy footprint, the operational, maintenance, and management resources, and the number of facilities
    - Using a pay-as-you-go pricing model for services on demand rather than procuring entire solutions
    - Leveraging existing DoD cloud computing development environments to reduce software development costs

- **Increased Mission Effectiveness**
    - Enabling access to critical information
    - Leveraging the high availability and redundancy of cloud computing architectures to improve options for disaster recovery and continuity of operations
    - Enhancing Warfighter mobility and productivity through device and location independence, and provision of on-demand, yet secure, global access to enterprise services
    - Increasing, or scaling up, the number of supported users as mission needs surge, optimizing capabilities for the joint force
    - Enabling data to be captured, stored, and published almost simultaneously, decreasing the time necessary to make data available to users
    - Enabling the ability to create and exploit massively large data sets, search large data sets quickly, and combine data sets from different systems to allow cross-system data search and exploitation

- **Cybersecurity**
    - Leveraging efforts such as FedRAMP that help standardize and streamline Certification and Accreditation (C&A) processes for commercial and Federal Government cloud providers, allowing approved IT capabilities to be more readily shared across the Department
    - Moving from a framework of traditional system-focused C&A with periodic assessments to continual reauthorization through implementation of continuous monitoring
    - Moving to standardized and simplified identity and access management (IdAM)
    - Reducing network seams through network and data center consolidation and implementation of a standardized infrastructure

Challenges the Department Faces Moving to a Cloud Computing Environment

Most DoD systems have been designed to operate in a protected environment with dedicated infrastructure, and though cloud computing continues to demonstrate significant benefits, challenges remain. The Department must be careful not to jeopardize its mission by trading the confidentiality, integrity, and availability of DoD information for desired benefits. The Department will ensure adherence to the National Continuity Policy (See Appendix B, (Reference H)) that requires communications/IT capabilities to maintain data availability and resilience to sustain Component mission- essential functions (MEF) and DoD's Departmental Primary MEF (PMEF) in support of National Emergency Functions (NEF).

Table 2 identifies five broad categories of challenges and mitigation activities that will help the Department meet those challenges. Note that these challenges are not exclusive to cloud computing and apply to all levels of the Department.

Table 2: Challenges Moving to a Cloud Computing Environment

Governance and Culture Changes	
Challenge	**Mitigation**
• Establishing and maintaining a DoD CIO- led Enterprise- First approach • Sustaining and managing the evolution of the Enterprise Cloud Environment to enable JIE objectives • Overcoming cultural roadblocks that make it difficult for the Department's IT community to adopt an Enterprise-First approach and cloud services approach • Incentivizing entrepreneurial innovation in the face of current regulatory DoD policy and process mandates	• Execute authorities delegated to the DoD CIO to approve/enforce an Enterprise-First cloud approach to JIE capabilities throughout the Department • Establish DoD CIO- led joint governance to oversee Component cloud-related activities • Establish comprehensive governance at Service CIO levels to oversee and guide implementation and execution • Execute a cloud awareness education campaign • Adopt Agile acquisition and funding mechanisms to exploit cloud innovation
Information Assurance, Resiliency, and Cybersecurity	
Challenge	**Mitigation**
• Achieving real-time visibility into all cloud activities where consumers do not have physical control over their systems, and the systems can change dynamically as providers respond to emergent capacity requirements • Implementing continuous monitoring, handling intrusion detection and alerts, and providing diagnosis and response • Ensuring communications/IT capabilities to	• Implement Information Assurance (IA) controls that provide real time monitoring to designated DoD IA personnel and provide methods and procedures for mission owners to request responses • Provide acquisition regulation and cyber defense policies to which cloud providers must adhere in order to adequately secure and defend DoD information

maintain data availability, privacy, and resilience • Maintaining forensic, records management, Freedom of Information Act (FOIA) reporting, and two-factor authentication with DoD Common Access Cards	• Implement new or adjust existing technical capabilities for operation within the cloud, and, in particular, provided to Department network and system operation centers (NOCs/SOCs) • Bolster critical infrastructure protection efforts to ensure a resilient and sustainable cloud computing environment • Implement IdAM, Public Key Infrastructure (PKI), and secure data tagging Department-wide • Ensure effective acquisition of commercial cloud services leveraging Federal CIO Councils, "Creating Effective Cloud Computing Contracts for the Federal Government" (See Appendix B,(Reference I)
Network Dependence at the Tactical Edge	
Challenge	**Mitigation**
• Providing access to reliable, remotely delivered services to Warfighters and support personnel operating in restricted tactical environments (high mobility, disconnected, intermittent connectivity, limited bandwidth and long latency) • Providing adequate protection to ensure continuity of operations and resiliency	• Deliver services as far forward as possible, using the least bandwidth possible while ensuring offline capabilities are maintained
Service Acquisition and Funding Sustainment	
Challenge	**Mitigation**
• Changing from a focus on the acquisition of materiel solutions to the acquisition and consumption of cloud services • Establishing funding mechanisms that can rapidly adapt to changing demand to sustain the growth of widely used services • Reducing or eliminating investment in underutilized and underperforming services • Implementing effective change management in a cloud environment • Ensuring data ownership and transportability of data from one cloud provider to another	• Establish policies and procedures for budgeting, funding, acquisition, and cost recovery that leverage a "fee-for-service" model • Use a cloud broker function to manage the use, performance, and synchronized delivery of cloud service offerings • Develop a budget strategy to fund initial cloud investments across the Department • Reduce or eliminate investment in underutilized and underperforming services • Establish and enforce DoD cloud computing change management criteria • Ensure contracting and acquisition mechanisms preserve data integrity and support data transportability

Data Migration, Management and Interoperability	
Challenge	**Mitigation**
• Ensuring that data and applications hosted in the various cloud services can be discovered, accessed, stored, used, and protected among various DoD components and mission partners • Providing adequate security services (monitoring and response, IA, etc.) to ensure the integrity, confidentiality, and availability of DoD data in a cloud computing environment • Ensuring that the hosting of DoD Component data by a cloud service provider is subject to technical and contractual conditions that facilitate migration of the data to another provider or back to the DoD Component • Ensuring data interoperability and secure information sharing with multi-national and other mission partners via cloud services • Ensuring data portability and interoperability • Ensuring all categories of Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), Personal Health Information (PHI), International Traffic in Arms Regulations (ITAR), and Contractual Information, are properly and adequately secured, controlled, and audited during transmission, processing, and storage	• Enable intelligent delivery of multi-source information in diverse application formats by providing seamless, real-time information sharing that is secure, supports multiple platforms, and combines new advances in information processing and data analysis • Enforce use of risk assessments that consider exposure to the legal, law enforcement, and national security requirements of the host country • Ensure Service Level Agreements (SLAs) are written to address DoD mission assurance and data confidentiality and availability requirements • Require and enforce the adoption of enterprise discover and search, enforcement of IdAM and data tagging, joint governance, and cross domain security solutions • Require the use of data portability and interoperability standards as they emerge • Enforce compliance with laws and regulations regarding CUI data

Transitioning to the DoD Enterprise Cloud Environment

The transition to cloud computing requires moving from the current state of duplicative, cumbersome, and costly application silos to an end state which is an agile, secure, and cost effective service environment that will enable Components to rapidly configure and deploy IT to meet changing mission needs. The transition will not be accomplished all at once, but in planned phases, building on the successes and lessons learned from DoD and Industry cloud initiatives as they are implemented.

The vision for the Department is a multi-provider Enterprise Cloud Environment that meets DoD IT objectives. Program managers and application/service owners will generally not need to design the physical infrastructure that hosts and runs their software applications. Instead, they will be responsible for designing and developing applications and services that operate within the computing environments offered by DoD data center providers. New Core data centers, and standards-based equipment deployed in regional and tactical data centers, will provide the

physical computing infrastructure to deliver data and cloud services to the user, regardless of access point or the device being used across the Global Information Grid (GIG). These data centers will host existing applications, provide a viable platform for the development of new applications, and enable shared hosted services.

The Department will be responsible for the Enterprise Architecture and standards that will guide how the DoD cloud is designed, operated, and consumed. The Enterprise Cloud Environment, in turn, will drive architectures and standards that extend the full range of IT services to mobile devices and to the tactical edge. The Enterprise Cloud Environment will provide Department-wide services at the enterprise level that enable improved interoperability, access, data integrity, and security. In addition to enterprise services provided Department-wide, Components will be encouraged to use or provide cloud services offered by other Components, other entities in the Federal government, mission partners and commercial vendors that meet their specific mission requirements. All services will comply with Department IA, cybersecurity, continuity and other policies.

The DoD Enterprise Cloud Environment will support new applications, access to legacy applications and data exchanges on NIPRNet, SIPRNet, and Top Secret Sensitive compartmentalized Information (TS SCI) security domains. This environment will be closely aligned with Intelligence Community initiatives and will support information sharing with DoD traditional and non-traditional partners on JWICS, the mission network, and other networks. The DoD CIO will lead NIPRNet and SIPRNet efforts while the Director of National Intelligence (DNI)/CIO will lead TS SCI and above.

Figure 1 is a logical depiction of the envisioned DoD Enterprise Cloud Environment end state. It illustrates that the DoD Enterprise Cloud is an integrated environment on the GIG, consisting of DoD Components, commercial entities, Federal organizations, and mission partners.

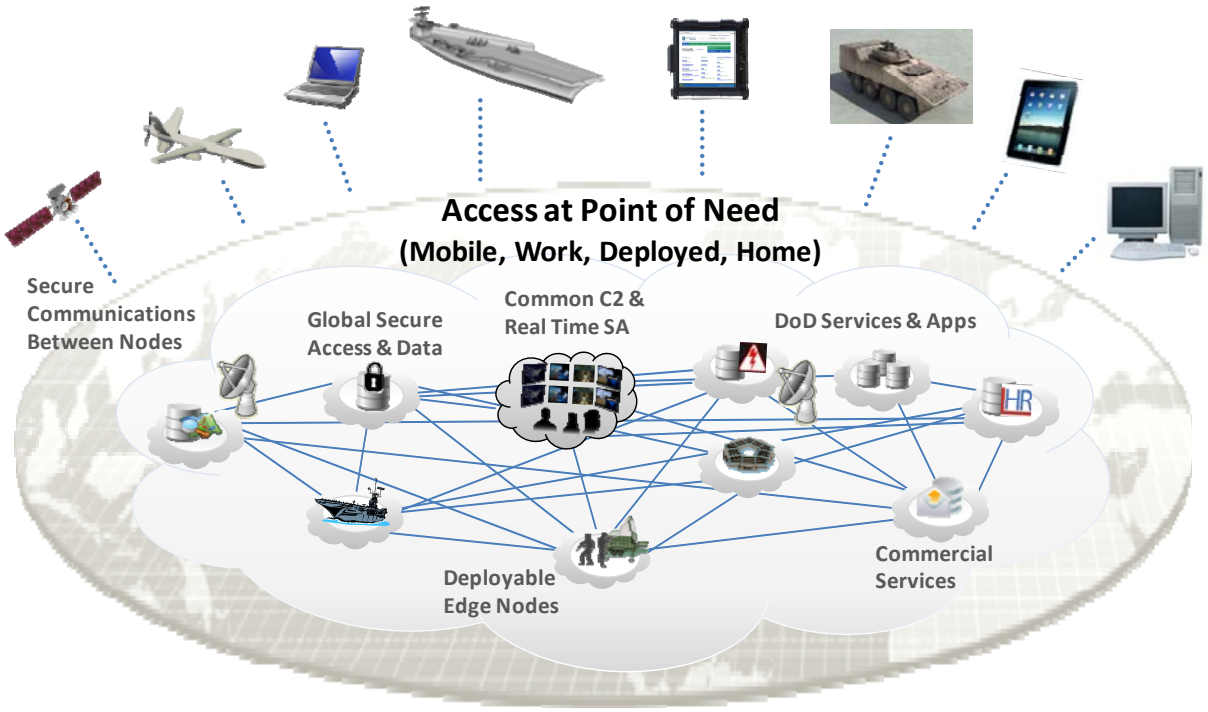


Figure 1: DoD Enterprise Cloud Environment

The Department has identified four concurrent steps that enable a phased implementation of the DoD Enterprise Cloud Environment:

Step 1. Foster Adoption of Cloud Computing by establishing a strong governance structure that has the authority and responsibility to drive an Enterprise-First approach and enable IT financial, acquisition, and contracting policy and practice reforms.

Step 2. Optimize Data Center Consolidation by implementing a limited set of standardized software platforms and data centers that will enable effective management as a single enterprise with a reduced intrusion surface for cyber threats.

Step 3. Establish the DoD Enterprise Cloud Infrastructure as the foundation for rapid participation in the DoD Enterprise Cloud Environment.

Step 4. Deliver Cloud Services using commercial service providers and continuing the development and implementation of DoD cloud services.

The following sections describe these steps in greater detail.

Step 1: Foster Adoption of Cloud Computing

IT Governance that establishes an Enterprise First approach to the funding, acquisition, creation, management and use of cloud services, through policy and process change, is

essential in fostering adoption of cloud computing. The DoD CIO will execute delegated authorities to approve/enforce an Enterprise-First cloud approach to JIE capabilities throughout the Department. The DoD CIO is committed to working with major stakeholders, such as the Defense Information Systems Agency (DISA), Joint Staff, and Military Department (MILDEP) CIOs, to implement an outreach and awareness campaign to expand the base of consumers and providers, and increase the visibility of available cloud services in other parts of the Government.

Govern the DoD Enterprise Cloud Environment

Comprehensive joint IT governance, led by the DoD CIO, will drive the changes necessary to transition to cloud computing. Enhanced governance processes and policy enforcement mechanisms will be instituted to manage the rapid evolution of cloud services within the Department, maximizing the potential value of cloud services and minimizing the risks. Strong governance mechanisms will support consistent interpretation of policy, monitor DoD enterprise cloud performance, and address cloud service consumer and provider issues.

DoD CIO- led governance will facilitate an enterprise approach to cybersecurity, continuity of operations, IA, resilience, and ensure that DoD's Enterprise Cloud Environment is compliant with all existing laws and regulations. The DoD Enterprise Cloud Environment will require rigid standards for how users are identified, transmission is assured, and resources (persons, organizations, groups and applications), are tracked.

Effective governance and collaboration with key Department leaders and stakeholders is necessary to establish policy and organizational process changes that will transform the way IT is acquired, operated, and managed. Coordination will occur outside the Department with stakeholders from the National Security Agency (NSA) others in the Intelligence Community and other Federal partners as they evolve their own cloud services.

Transition to cloud computing may require upfront investments and realignment of planned IT roadmaps. The Department will use business case analysis to determine best value between alternatives, and will define an investment management process that enables the rapid evolution of enterprise cloud services and prevents non-standards-based IT service silos from proliferating within the Enterprise Cloud Environment.

The Department's IT governance must ensure alignment of DoD investments, including Program Objective Memorandum (POM) activities, policies, processes and standards that will enable a transition to cloud computing. The Department will exercise governance mechanisms to ensure cloud computing options are analyzed during the course of DoD budget and acquisition processes for each IT capability development initiative in compliance with OMB guidance (See Appendix B,(Reference J). A Component's decision to move data to a cloud computing service

will balance benefits and risk, measured against DoD mission assurance and data confidentiality requirements. These assessments and approvals will be conducted in accordance with Federal laws and regulations governing the protection of Government information, and DoD IA and information security policies.

Comprehensive governance processes will promote and enable the use of standardized SLAs that facilitate the adoption of shared services and virtual computing resources for mission and support functions. SLAs must define performance with consistent and clear terms and definitions and demonstrate how performance will be measured. Governance will define the enforcement mechanisms that should be in place to ensure SLAs are met. The Department will drive efficiencies by using Commercial business models, ensuring competition and setting new performance standards, targets, and metrics, as well as monitoring and reporting progress.

Adopt an Enterprise First Approach

Higher flexibility, lower costs, improved quality of service

The Enterprise First approach is a cultural shift to transform DoD from a coalition of Departments and Agencies with their mission-specific sets of systems, processes, governance, and controls to a more seamless, coordinated, unified, and integrated data-centric enterprise information environment. The Department's efforts in general will be directed to reduce reliance on non-shareable, dedicated infrastructures. Components will be incentivized to rely on shared, virtualized infrastructure through a utility or cloud computing delivery model. Legacy IT systems will be migrated to a shared computing capability wherever practical.

Adopting an Enterprise First approach will reduce the acquisition and maintenance of dedicated, program-specific resources. The desired outcome is the transformation of the Department to an Enterprise Cloud Environment with common standards, consolidated cybersecurity, continuity of operations, IA, resilience, and centralized governance.

Reform DoD IT Financial, Acquisition, and Contracting Policy and Practices

Change the rules and make it happen

Today's delivery and operation of a DoD Enterprise Cloud Environment is hampered by existing policies and processes that were implemented to support traditional IT acquisition. The Department's typical acquisition approach bases investment decisions on significant investigation of capability needs, requirements definition, analysis of alternatives (AoA), and system growth projections. This works in an environment with relatively fixed requirements, known future needs, and static technology, but does not accommodate a multi-provider cloud environment. The Department must alter this acquisition approach if it expects to keep pace with IT advancements and achieve the efficiencies these advancements represent. To accomplish this, the Department must:

Streamline Key DoD Processes to reduce Operations and Maintenance (O&M) costs by leveraging economies of scale, and automate monitoring and provisioning to reduce the human cost of service delivery and assurance.

Change Acquisition and Contracting Models to reduce acquisition complexity; shift the DoD mindset from acquiring and managing IT assets (materiel solution development) to providing and consuming services; and support new funding, contracting, and acquisition models for agile solutions.

Publish Guidance and Policies that support transition to, and use of, cloud services.

The Department has initiated efforts to develop JIE requirements for cloud services that can use incremental investments and fee-for-service models rather than large-scale, up-front investments. New and innovative funding mechanisms are needed that can rapidly adapt to changing demand and sustain the growth of popular services. Services already developed by the Components for their use could be extended and shared across the Department. As efficiencies are gained through data center consolidation, some savings may resource additional cross-service investments. Periodic value assessments will drive additional investments and iterative refinements. To accomplish the needed change, the DoD CIO will work with the following organizations to update related policies and processes:

- USD (Policy) to update:
  - POM guidance and the POM issue process for enterprise cloud services
- Joint Staff to modify:
  - Joint Capabilities Integration and Development System (JCIDS)/Capabilities Requirements Process documentation (Chairman of the Joint Chiefs of Staff Instruction (CJCSI)) (See Appendix B,(Reference K)).
  - Interoperability of IT and National Security Systems (NSS) (See Appendix B,(Reference L))
- USD (Acquisition, Technology, and Logistics) to modify or establish:
  - Provisions in the Defense Acquisition System (DAS) (See Appendix B,(Reference M)) that ensure the consideration of the use of enterprise cloud services as a mandatory element of the AoA
  - Business Capability Lifecycle process
  - New standard contract clauses and any accompanying changes necessary to the Defense Federal Acquisition Regulation Supplement (DFARS)
- USD(Comptroller)/CFO and DCAPE to modify or establish:
  - Planning, Programming, Budgeting and Execution (PPB&E) (See Appendix B,(Reference N))
  - New Program Element and budget line item resources

    - Increased visibility within authoritative DoD resource databases
    - Establish new contracts and contracting vehicles
- DoD Comptroller and CFO to:
    - Revise PPB&E regarding enterprise cloud services and establish provisions in the DoD Financial Management Regulation
    - Address appropriate resourcing methodologies and sources for funding cloud services and migrations
- DCMO to align Business Mission Area policies and procedures.

Implement a Cloud Computing Outreach and Awareness Campaign

The greatest impediment to the successful adoption of cloud computing is not technological in nature, but rather, the set of cultural roadblocks that make it difficult for the Department's IT community to adopt a new technology. As with any significant change, the move to the cloud requires a shift in mindset to accept new ways of creating solutions and an informed workforce to enable acceptance and use of cloud services.

The DoD CIO will implement a cloud computing outreach and awareness campaign to gather input from the major stakeholders, expand the base of consumers and providers, and increase visibility of available cloud services throughout the Federal government. Current cloud-related activities will provide input to the development of cloud computing planning and implementation guidance. Specifically, these activities will inform the Department on the key benefits and challenges of cloud services, including value propositions, security features and challenges, sample mitigation strategies, training, lessons learned, and case studies. This outreach will include:

- Identifying best practices to guide stakeholders in the adoption and implementation of cloud services, including the acquisition and provisioning process and identifying and evaluating associated compliance and legal issues
- Establishing methodologies to enable effective assessment and implementation of cloud services, including consideration of maturity, cost recovery, security compliance, etc.
- Identifying challenges and recommending mitigations to resolve them
- Identifying metrics and performance measures that demonstrate successful migrations and use of cloud services
- Identifying and assessing new and evolving technologies in the marketplace and providing feedback on the maturity of these offerings
- Providing specific skills training for acquisition and contracting specialists for agile IT procurements, including cloud computing. IT program managers must also acquire the skills needed to make informed decisions regarding existing and planned cloud services

- Emphasizing individual and organizational responsibility to assess and manage risks associated with cloud computing

Step 2: Optimize Data Center Consolidation

In August 2010, the Secretary of Defense directed the consolidation of IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs, and to improve the DoD's ability to execute its missions while defending its networks against growing cyber threats. In response, the Department has identified opportunities to consolidate DoD IT infrastructure through several initiatives, one of which is data center and server consolidation. As identified in the JIE, enterprise data center consolidation involves Component applications and data transitioning to Core data centers and the DoD Enterprise Cloud Environment.

The Department will reduce the hardware footprint in data centers by implementing server virtualization and Infrastructure-as-a-Service. In addition, DoD will reduce software redundancy and increase interoperability through the implementation of a limited set of standardized software platforms that are continuously monitored and respond to emerging threats. Optimizing data center consolidation will facilitate standardization across data centers in the way they deliver services to users and the internal processes used to manage the business operation. Consolidation will not only reduce the cost of data center infrastructure, but will enable effective management as a single enterprise with a reduced intrusion surface for cyber threats. Combining the establishment of core cloud infrastructure with data center consolidation will establish the federation and standardization of Core data centers for the DoD.

Consolidate and Virtualize Legacy Applications and Data

Consolidating data centers throughout the Department into a smaller, core data center infrastructure will reduce the number of different hardware platforms, which will result in an eventual savings in equipment, facility, and operational costs. Although core data centers may be operated by different organizations within DoD, they will all operate according to standard operational, business, and IT Service Management processes to ensure that they function as a single, logically seamless computing environment meeting all requirements for graceful fail over, disaster recovery, continuity of operations, security, resiliency, and load balancing.

The consolidated data centers will be guided by the NIST Cloud Computing Reference Architecture, and the NIST Cloud Computing Standards Roadmap. Leveraging the NIST guidance, a DoD Cloud Reference Architecture will include modular infrastructure that will scale up for deployment within large, Continental United States (CONUS) data centers and scale down to offer containerized and small footprint computing resources in regional facilities and deployed tactical edge environments.

Through virtualization, data centers will focus on hosting existing applications and providing a viable platform for the development of new applications and sharing hosted services. The enterprise cloud architecture and standards will extend the full range of IT services to mobile devices and to the tactical edge. As legacy applications are migrated and new applications are produced, each will gain "built-in" features, such as support for multi-data center replication, "follow-me" data that automatically moves to where it is needed, and intelligent information services that leverage news and data available across the Department.

The DoD ITESR identifies data center, network and server consolidation for the GIG computing environment as key initiatives. Through consolidation and virtualization, the Department will develop a DoD enterprise cloud platform that meets several objectives of the DoD ITESR including delivering services to the tactical edge. Consolidation and virtualization will enable access to reliable, remotely delivered services to Warfighters and will support personnel operating in restricted tactical disconnected, intermittent and low-bandwidth (DIL) environments from any device, anywhere and anytime. Smart replication will ensure that clustered information automatically migrates to nearby resources. Use of the latest standards for offline data storage and applications will support specified mobile and desktop platforms. End-users will access virtual servers that have been allocated to provide client-side applications and services supporting multiple information-domain access.

Virtual Desktop Infrastructure (VDI) initiatives will reduce desktop capital, maintenance, and management costs. These efforts will reduce time to deliver new end-user capabilities and shorten cycle time for upgrades through increased automation efficiencies requiring less support and facilitating compliance with DoD standards and policy.

DoD will realize savings by keeping hardware, software and operations as consistent and standardized as possible, while also reducing the number of tools, activities and personnel needed to perform the same basic functions. A portion of the savings that results from consolidation and standardization could go towards funding the delivery of these services, either at the Component level or at the Enterprise level; however, potential efficiencies may not be automatically realized without added resources.

Step 3: Establish the DoD Enterprise Cloud Infrastructure

The Department will provide an enterprise cloud infrastructure that is resilient and operates seamlessly between all DoD Components. This enterprise cloud infrastructure will be incorporated into core data centers and is the "engine" behind the DoD Enterprise Cloud Environment. An essential part of the cloud infrastructure is cloud service brokerage which makes it easier, safer, and more productive to navigate, integrate, consume, extend and maintain cloud services, particularly when they span diverse Department, Federal and

commercial cloud service providers. Additionally, the cloud infrastructure facilitates Agile methods and will provide a test and development environment to enable rapid service delivery. Cloud computing can offer a highly resilient computing environment that does not have a single point of failure. The failure of one node of a system in a cloud environment should have no impact on overall information availability, reducing the risk of perceivable downtime. The DoD Enterprise Cloud Infrastructure must ensure the security of data and information by reducing the complexity of the information environment and making certain that all DoD Computing Service Provider environments operate at the minimum acceptable standards outlined within current DoD policy and technical guidance.

Incorporate Core Cloud Infrastructure into Data center Consolidation

The foundation for rapid participation in the DoD enterprise cloud environment

Incorporating cloud infrastructure into Core data center data centers provides benefits beyond those achieved through data center consolidation alone. As core data centers are established, cloud functions such as IaaS, SaaS, PaaS, and content caching will be added. Core data centers will meet Exemplar data center standards supporting cloud-based Enterprise Services serving a global user-base. Optimized Core data centers with "Cloud-ready" infrastructure will enable secure, highly scalable applications to be rapidly developed, deployed, and continuously improved while hosting those legacy applications and systems that are still vital to the DoD mission.

Figure 2 illustrates the transition from today's environment to consolidated and virtualized applications and data, and finally to a cloud infrastructure that enables the Department's move to a cloud computing environment.

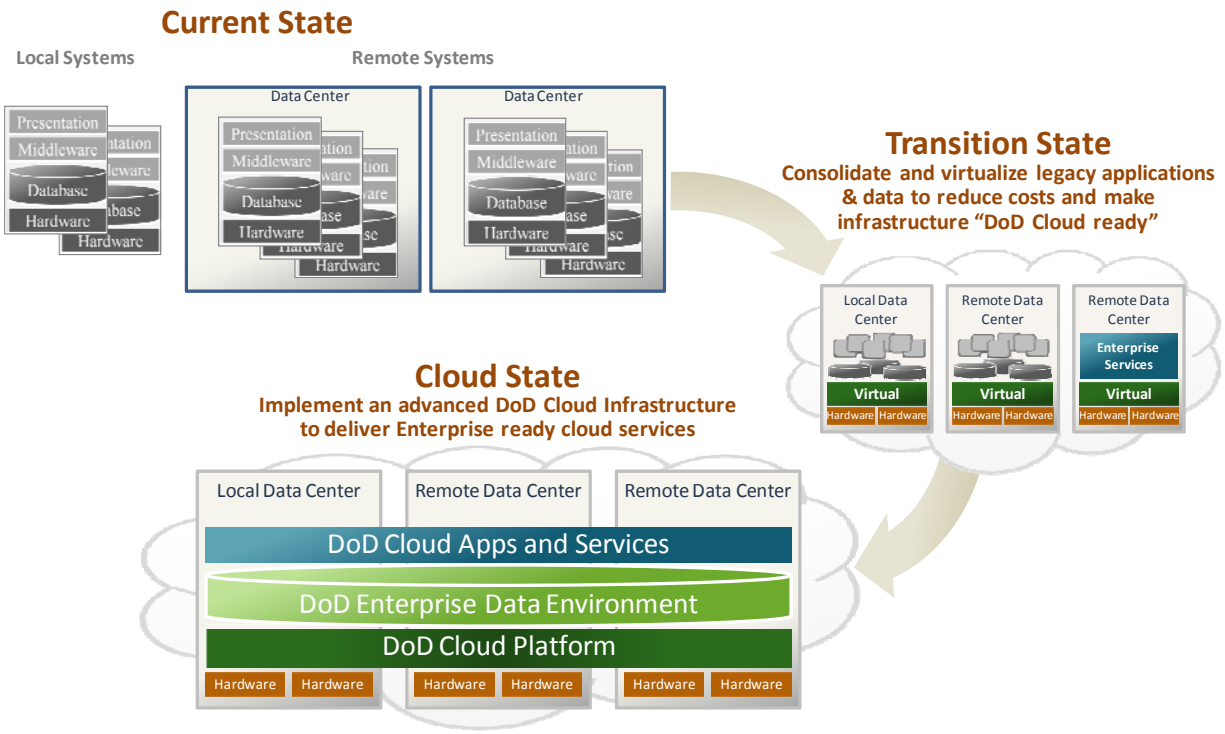


Figure 2: Consolidated Core Data Centers will Form the Basis of the Enterprise Cloud Infrastructure

Optimize the Delivery of Multi-provider Cloud Services via Cloud Service Brokerage

The Enterprise Hub for runtime selection, integration and delivery of services

To sustain an integrated and optimized multi-provider cloud environment, a Cloud Service Broker with both a technical and an organizational component is needed to manage the use, performance, and synchronized delivery of cloud service offerings within the Department, from other Federal, and commercial providers. The broker will enable DoD organizations to tailor the availability and delivery of cloud services based on technical and mission requirements. For example, rather than each DoD organization monitoring service provider performance and security controls, the broker will be the central point for integrating this information from each of the providers and making it available to the various DoD stakeholders. Moving beyond the ability to match potential consumers with the best services to meet their needs, the broker will provide an integrated set of capabilities that each DoD organization would have had to deliver. Some of these capabilities include:

- Ensuring compliance with DoD IA requirements for encryption and key management integration with DoD's emerging IdAM services
- Enabling integrated cyber intrusion detection and response
- Enabling a common entry into the cloud - the DoD cloud service storefront
- Providing an integrated billing and contracting interface
- Managing integrated service delivery from DoD and commercial service providers
- Providing integrated identity and access controls and integration with DoD's emerging IdAM services
- Controlling usage and optimizing cloud workload distribution
- Maintaining configuration control and compliance of DoD resources deployed into the cloud
- Ensuring that providers maintain DoD standards and architectural compliance
- Enabling continuous monitoring and reporting on performance of SLAs and IA controls
- Providing a common, integrated help desk

Starting with a simple online catalog of DoD cloud services, the Cloud Service Broker function will grow to enable DoD customers and organizations to tailor the set of available services and optimize the cloud performance based on their technical and mission requirements.

Use Agile Approaches to Drive Continuous Service Innovation

Eliminates obsolescence at the time of delivery

The effective delivery of DoD-provided cloud services will require the Department to transition from an acquisition process focused on acquiring materiel solutions to one focused on operating, and continually enhancing, services. Use of Agile processes will enable rapid and continuous service improvement in response to changing mission needs. The Department will establish a consolidated, enterprise development and test cloud environment, provided by Components, to enable continuous delivery and integrated DevOps. This test and development cloud environment will enable applications and services to run in a distributed environment, reducing time to deliver content to clients.

> *"**DevOps**" is an emerging set of principles, methods, and practices for communication, collaboration and integration between software development (application/software engineering) and IT operations (systems administration/infrastructure) professionals*

This cloud development and test environment will:

- Enable agile development and continuous enhancement of DoD- provided cloud services that will rapidly respond to changing user needs, technologies, and threats
- Facilitate the optimal migration and integration of legacy systems into the cloud environment
- Reduce duplicative hardware and software expenses necessary to support a development program
- Enable the provision of automated assembly and test of software systems
- Incorporate additional development and test services provided by DoD Components and commercial providers
- Include an integrated set of services to include automated on-demand provisioning of development and test cloud resources
- Enable the integration of identity management

Exploit Cloud Innovation to Drive Secure Information Sharing

Increased Decision Superiority through data intensive analytics

The Enterprise cloud infrastructure will enable a data-centric approach to the development and implementation of cloud services. The deployment of standardized data interfaces within the cloud will allow users anywhere to retrieve, scrub, and sanitize data on demand over a vast array of protocols and technologies. The cloud infrastructure will facilitate managing the rapidly increasing amounts of data. Innovative data cloud services will deliver actionable information. The Department will leverage and align with IC cloud services.

Operational Data Functions and Informational Data Services

The Department is taking a data-centric approach to cloud services, and will securely architect for interoperability. Improving the quality, accessibility, and usability of DoD data through well-defined standards will include the use of machine-readable formats such as web services and common metadata tagging schemas.

The NIST Cloud Computing Reference Architecture identifies the importance of data and common data functions as key underpinnings of cloud computing. While the reference architecture is still evolving, NIST currently separates data functions into two categories: operational data functions and informational data services.

Operational data functions include activities such as data tagging, data integrity, data security, data portability, data transport, data presentation, data maintenance, and file management. Operational data functions support the manipulation, extraction, and presentation of meaningful results to end users, and are primarily used and maintained by the cloud provider.

Informational data services enable the aggregation or the mash-up of multiple data sources located in data centers across the globe into a correlated purposeful data set supporting a user's mission needs. Data services can be defined as a set of computing services exposing informational data in a way that adhere to cloud computing reference architecture – stand-alone or within a system of systems. These services are useful to end users because of the standardized format and methodologies that allow them to access and work seamlessly with the information.

NIST currently maps informational data services to the SaaS and PaaS layers, and operational data services to SaaS, PaaS, and IaaS layers.

Data as a Service (DaaS)

Because of the huge impact that cloud computing can deliver to improve DoD data and information management, the DoD Cloud Computing Strategy diverges from the NIST cloud service model definitions to uniquely identify DaaS and the resulting DoD Data Cloud as key concepts. Within the DoD, DaaS encompasses two primary activities. The first is the continued implementation of the DoD Data Strategy and deployment of standardized data interfaces that make DoD information visible and accessible to all authorized users. The second is the incorporation of emerging "big data" technologies and approaches to effectively manage rapidly increasing amounts of information and deliver new insights and actionable information.

Embracing Cloud-Based Data Technologies

While relational databases and data warehouses have dominated the data environment for the past quarter century, these traditional technologies are ill-suited to the new challenges being faced as data storage requirements begin to approach quadrillions of bytes (petabytes). As the volumes of unstructured and structured data sets proliferate, our ability to capture and effectively process this information has not kept pace. The complexities of capture, store, index, and access of large data stores have made it difficult for the Department to fully leverage our increasing volumes of data and information.

Cloud computing technologies such as noSQL databases (e.g., Google's Big Table and Apache's Hadoop/HBase) and parallel computing clusters provide new capabilities to manage large, diverse data sets, enable new data transformation methods and enable advanced analytics. Department data clouds based on these technologies would enable elastic scaling, distributing the data across multiple hosts as load increases; improve data management economics by using clusters of cheap commodity servers rather than expensive proprietary servers and storage systems; implement flexible data models that would allow applications to easily store virtually any data type or structure without major modifications; and operate on a dynamic and resilient

data platform that automatically distributes and synchronizes data across DoD's varied mission environments.

Data transport and cloud-to-cloud Interoperability entail moving data and applications of varying size and complexity from existing desktops to the cloud while ensuring data, applications and services hosted within the enterprise cloud environment are compatible so that information can move freely. Data retrieval and viewing benefits from a cloud approach by presenting data from its source location rather than transporting it across the Internet. By contrast, cross-domain services are essential to achieving DoD IT objectives and the enterprise cloud environment and will require more robust security controls to ensure that classified information is not compromised between high and low security domains.

Step 4: Deliver Cloud Services

The Department will build on its enterprise services efforts and continue to deliver DoD Cloud services that provide improved IT capabilities at reduced costs. Components will be encouraged to use Enterprise Services, shared services (cloud services offered by other Components, the Federal Government, mission partners) and commercial vendors that meet their specific mission requirements. The Department will revise IA policies, standards, and processes to enhance the reliability and security posture of DoD and commercial cloud services.

Continue to Deliver DoD's Enterprise Cloud Services

"Load and Run" enterprise-ready, field deployable application services

Currently, DoD consumers have access to several cloud services, including services which are provided by DISA and hosted in DoD enterprise data centers, a few of which are:

- Defense Connect Online (DCO)
- Global Content Delivery Service (GCDS)
- Forge.mil development platform tools
- RightNow Customer Relationship Management (CRM) tools
- Rapid Access Computing Environment (RACE) for processing resources

Continuing to deliver the existing services above and developing and offering the following enterprise services via the DoD Enterprise Cloud Environment will support meeting the Department's IT objectives:

- **Engineer Global Federation Approach:** The Department will engineer a global federation approach to support central management and full interoperability across multiple clouds operated by the Components within the DoD Enterprise Cloud Environment

- **Enterprise File Storage:** The Department will implement enterprise file storage as a capability to enable global access to data and files by an authorized user, from anywhere and from any device
- **Enterprise Directory Services:** The Department will implement enterprise directory services to make data visible, discoverable, and accessible
- **Unified Capabilities:** The Department will migrate legacy voice, video and data collaboration services to everything over IP (EoIP); standardize and consolidate Component IP convergence efforts across DoD to reduce cost and streamline management; enhance wireless and mobility support; and provide real-time collaboration (assured, integrated voice, video, and data services)
- **Cross-Domain Solution as an Enterprise Service**: The Department will develop the enterprise-level, cross-domain solutions required to fulfill emerging capability needs and user requirements across the DoD. DISA will continue to employ a diverse best of breed fleet of cross-domain technologies.
- **Enterprise Messaging and Collaboration**: The Department will provide a set of Enterprise Messaging and Collaboration capabilities that includes, at a minimum, instant messaging (IM), chat, email, portal, and web conferencing. Other capabilities to be provided facilitate data tagging and records management. These capabilities enable information sharing from any device attached to a DoD network.
- **Identity and Access Management (IdAM) Services**: The Department will implement enterprise-wide IdAM services that are focused on managing digital identity, credentialing and authenticating users, authorizing access to resources, and using data tagging to support and enforce access control policies throughout the enterprise.

The Department will continue to improve these services, provide additional cloud services, and incorporate cloud services provided by individual DoD components as they emerge.

Leverage Externally Provided Cloud Services

A bigger toolbox for our Warfighters

The Department's Enterprise Cloud Environment will provide Department-wide services at the enterprise level that enable improved interoperability, access, data integrity, and security. In addition to Enterprise Services provided Department-wide, Components will be encouraged to use or provide cloud services offered by other Components, other entities in the Federal Government, mission partners and commercial vendors that meet their specific mission requirements while complying with Department IA, cybersecurity, continuity, and other policies.

With the emergence of FedRAMP and the increasing maturity of commercial cloud services, there is increasing potential to leverage commercially provided services to support the Department's IT requirements. However, the increasing volume and sophistication of cyber intrusions on the Internet bring significant risks to the Department's mission. Moving DoD information into commercially provided clouds that operate outside of DoD security protections and operational control can increase these risks.

IA Policies, Standards, and Processes

The Department recognizes the significant improvements in cybersecurity achieved by commercial industry as cloud computing continues to mature. However, serious threats remain to DoD information and information systems that can have adverse impacts on the Department's mission, individuals, other organizations, and the Nation. Cyber intrusions on DoD information systems today are often aggressive, disciplined, well-organized, well-funded and very sophisticated.

The Department is currently revising the DoD 8500 series (See Appendix B,(Reference O)) and adopting NIST SP 800-53 security controls and NIST SP 800-53a assessment procedures (See Appendix B,(Reference P)) while coordinating with industry and academia to enhance the reliability and security posture of DoD cloud services. The standardization of IA controls and sharing of security assessment data through the FedRAMP program will facilitate the adoption of commercially provided cloud services based on risk management that aligns DoD IA processes with those used elsewhere within the Federal Government.

These enhancements to the Department's IA policies and processes are designed to ensure that protection measures are applied commensurate with the system's criticality and sensitivity. Emerging processes will enable greater flexibility in determining appropriate priorities for agency information systems and subsequently applying the proper measures to adequately protect those systems. This will allow the Department to balance the importance of information resources against cybersecurity solutions and operations available within the Department or from commercial cloud providers. Where commercial services offer the level of protection necessary for a particular DoD mission and information set, the DoD will be able to leverage those commercially offered services and focus its own cybersecurity resources on more critical challenges.

An essential component of the ongoing, dependable use of externally provided cloud services is the integration of a cloud provider's continuous monitoring and response capabilities with USCYBERCOM's systems for protecting DoD information and ensuring DoD mission assurance with the Federal Information Security Management Act (FISMA) compliance and the Committee on National Security Systems Instruction (CNSSI) 1253 (See Appendix B,(Reference Q)). This

integration is needed to synchronize cyber intrusion detection, diagnosis, mitigation, and response activities, and maintain ongoing assurance of DoD information and mission.

Low Risk

DoD will begin using commercial cloud providers to initially support low risk information and mission functions. Data with confidentiality, integrity, and availability ratings that are FISMA low do not present significant impacts on mission effectiveness or operational readiness. This level consists of systems handling non-sensitive information necessary for the conduct of day-to-day business, but it does not materially affect support to deployed or contingency forces in the short term. This approach will enable the Department to rapidly mature its processes for using commercial cloud services while minimizing the potential impact to DoD operations and assets if confidentiality, integrity, or availability is lost. Because successful intrusions on DoD information systems can result in serious damage to the interests of the United States, the Department will take a cautious approach to using commercial cloud services. For instance, the same visibility into the real-time use, traffic, and consumption of data or information within DoD environments is required from commercially provided cloud services providing comparable services.

Moderate Risk

In addition to using commercial cloud providers to support low risk information and mission functions, commercial cloud services that meet FedRAMP moderate control levels will be candidates for inclusion in the Department's multi-provider cloud environment. This level of risk requires additional IA safeguards to mitigate possible loss of integrity, delay or degradation in providing important support services or commodities that could seriously impact mission effectiveness or operational readiness.

The Department will standardize and streamline the processes to support the migration of moderate risk data and information (e.g., CUI, PII, PHI, ITAR, and Export Administration Regulations (EAR)) to commercial cloud services. The Enterprise Cloud Service Broker will enable DoD Components to use commercial cloud services that meet FedRAMP low and moderate control levels, and make them available to other DoD Components through standardized contracts and leveraged authorization packages. The Enterprise Cloud Service Broker will ensure compliance with Department IA and cybersecurity policies to include the ongoing secure configuration, continuity, resiliency, and operations of these externally provided services, and help integrate commercial computer network defense operations with USCYBERCOM defense operations. In addition, the Department will be able to effectively execute its service consumer IA responsibilities.

High Risk

To ensure DoD mission success in the face of cyber degradation, loss, or intrusion, the Department will not use commercial cloud services when the loss of information confidentiality, integrity or availability could be expected to have a severe or catastrophically adverse effect on organizational operations, organizational assets or individuals. Protecting mission -critical information and systems requires the most stringent protection measures including highly classified tools, sophisticated cyber analytics, and highly adaptive capabilities that must remain within the physical and operational control of the Department. The Department will not use commercial cloud services that are generally available to the public and remain outside of DoD operational control to support high risk information and missions.

Next Steps

The DoD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE success. Detailed cloud computing implementation planning has been ongoing and informs JIE projected plan of actions and milestones in Capabilities Engineering, Operation and Governance efforts.

The DoD CIO will establish a joint enterprise cloud computing governance structure to drive the policy and process changes necessary to transition to the DoD Enterprise Cloud Environment and oversee the implementation of the DoD enterprise cloud strategy. This Senior IT Governance will provide the leadership to enable the DoD CIO's 10 Point Plan for IT Modernization and JIE efforts by:

- Ensuring the Enterprise Cloud Environment is a fundamental aspect of IT strategic planning, capital investment planning, cybersecurity, investment management, and systems acquisition, development and integration
- Defining the IT governance framework/organizational construct (working groups, etc), to review and monitor pertinent reference architectures and implementation planning to ensure coordinated and optimized consolidation efforts and the required cloud capability transitions/acquisitions, including test labs and pilot initiatives
- Publishing a DoD Policy to address the challenges associated with commercially provided cloud services and an Enterprise Cloud Security Framework that includes expanded risk assessment/risk management methodologies
- Establishing an Enterprise Cloud Service Broker to provide the additional integration, protections and ongoing monitoring needed to mitigate risks and achieve DoD requirements for cloud services
- Engaging with key Department process owners to establish agile acquisition and funding mechanisms that provide incentives for entrepreneurial innovation

- Establishing standardized, baseline DoD cloud computing SLAs and contract requirements to accommodate a multi-provider cloud service environment
- Identifying and reporting performance measures/metrics
- Establishing communications and training to continually drive cloud computing, and socialize new and updated business requirements, cloud computing successes, and lessons learned.

Conclusion

This strategy is intended to drive the Department toward changes required to dramatically improve the delivery and operation of IT, via an enterprise cloud environment, that provides tangible benefits to the DoD community. The Department's initiatives to achieve JIE goals and IT efficiencies in this current fiscal environment, and Federal mandates, accelerate this change.

There will be many benefits to moving applications and data to the cloud, but there are substantial risks. The Department has specific cloud computing challenges that require careful adoption considerations, especially in areas of IA and cybersecurity, continuity of operations, and resilience. Service acquisition and funding sustainment, data migration and management, and overcoming network dependence at the tactical edge are also challenges that need to be addressed to ensure objectives can be met.

The Department's approach to deliver an enterprise cloud computing strategy will require strong governance authority and continued commitment to greater transparency through regular and open reporting. Optimizing data center consolidation efforts with core cloud infrastructure must be carefully executed. To achieve the cloud computing goal, all barriers to consolidation and transition must be addressed without major delay. Governance must ensure mechanisms are in place to coordinate enterprise activities across the Department. Working with other key Department leaders, the DoD CIO will help establish funding models to sustain the development of Core shared data center infrastructure and the Enterprise cloud environment. DoD CIO will be the final decision authority and will provide oversight for Component execution of data center and server consolidation, exercising appropriate governance to ensure efficient orchestration of change.

The DoD CIO will continuously seek to refine and mature the cloud computing approach and maintain open communications with all levels of the Department, other Federal Agencies and our industry partners. Active participation and commitment of all DoD Components, in collaboration with the DoD CIO, is critical to ensure consistency, optimize benefits, and achieve the goal of this strategy.

APPENDIX A

Acronym List

AoA	Analysis of Alternatives
AT&L	Acquisition, Technology, and Logistics
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNSSI	Committee on National Security Systems Instruction
CONUS	Continental United States
CRM	Customer Relationship Management
CUI	Controlled Unclassified Information
DaaS	Data as a Service
DAS	Defense Acquisition System
DCAPE	Director Cost Assessment and Program Evaluation
DCMO	Deputy Chief Management Officer
DCO	Defense Connect Online
DFARS	Defense Federal Acquisition Regulation Supplement
DIL	Disconnected, Intermittent and Low-bandwidth
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
EAR	Export Administration Regulations
EoIP	Everything Over Internet Protocol (IP)
FDCCI	Federal Data Center Consolidation Initiative
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GCDS	Global Content Delivery Service
GIG	Global Information Grid
IA	Information Assurance
IaaS	Infrastructure as a Service
IdAM	Identity and Access Management
IM	Instant Messaging
IP	Internet Protocol
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITESR	IT Enterprise Strategy and Roadmap
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
JIE	Joint Information Environment

JWICS	Joint Worldwide Intelligence Communications System
MEF	Mission Essential Functions
MILDEP	Military Department
NDAA	National Defense Authorization Act
NEF	National Emergency Functions
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOC	Network Operation Centers
NSA	National Security Agency
NSS	National Security Systems
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OUSD	Office of the Under Secretary of Defense
PaaS	Platform as a Service
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMEF	Primary Mission Essential Functions
POM	Program Objective Memorandum
PPB&E	Planning, Programming, Budgeting and Execution
RACE	Rapid Access Computing Environment
SaaS	Software as a Service
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SOC	System Operation Centers
TS SCI	Top Secret Sensitive Compartmentalized Information
UDCMO	Unified Cross Domain Management Office
USD	Under Secretary of Defense
VDI	Virtual Desktop Infrastructure

APPENDIX B

References

A. **Federal Cloud Computing Strategy**, Feb 2011
http://www.cio.gov/documents/Federal-Cloud-COmputing-Strategy.pdf

B. 2012 National Defense Authorization Act (NDAA), Public Law 112-81
http://armedservices.house.gov/index.cfm/ndaa-home?p=ndaa

C. **Secretary of Defense Efficiencies Initiative**, Gates, Robert M., (2010), Statement on Department Efficiencies Initiative
http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1496

D. Office of Management and Budget (OMB)-directed **Federal Data Center Consolidation Initiative** (FDCCI)
http://www.cio.gov/pages-nonnews.cfm/page/The-Federal- Data center-Consolidation-Initiative

E. **OMB, 25 Point Implementation Plan** to Reform Federal Information Technology Management, December 9, 2010
http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

F. **Federal Risk and Authorization Management Program** (FedRAMP)
http://www.fedramp.gov

G. Department of Defense (DoD) **Information Technology (IT) Enterprise Strategy and Roadmap**, Version 1.0, September 6, 2011

H. **HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-20,** Subject: National Continuity Policy

I. **Creating Effective Cloud Computing Contracts for the Federal Government**, February 24, 2012 http://www.cio.gov/cloudbestpractices.pdf

J. OMB Circular A-11, "**Preparation, Submission, and Execution of the Budget**" of August 2011
http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2011.pdf

K. Chairman of the Joint Chiefs of Staff Instruction 3170.01G, **Joint Capabilities Integration and Development System** (JCIDS), March 1, 2009 (http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf

L. DoD Directive 4630.5 **Interoperability of IT and NSS**, May 5, 2004, certified cCurrent as of April 23, 2007 http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf

M. DoD Directive 5000.01,"**The Defense Acquisition System**", May 12, 2003 http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf

N. DoD Directive 7045.14, "**The Planning, Programming, and Budgeting System**", May 22 1984, Certified Current as of November 21, 2003 http://www.dtic.mil/whs/directives/corres/pdf/704514p.pdf

O. DoD Directive 8500.01E, "**Information Assurance** (IA)" (http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf)

P. **NIST Special Publications**

- [SP 500-292] NIST Cloud Computing Reference Architecture, September 8, 2011
- [SP 500-291] NIST-SP 500-291, NIST Cloud Computing Standards Roadmap, August 10, 2011
- [SP 500-293] NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap, (DRAFT) Release 1.0
- [SP 800-145] NIST Definition of Cloud Computing, September 2011
- [SP 800-53] NIST Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- [SP 800-53a] NIST Guide for Assessing the Security Controls in Federal Information Systems

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html

NIST FIPS Publications are available at: http://csrc.nist.gov/publications/PubsFIPS.html

Q. National Security Systems Instruction (CNSSI) 1253, **Security Categorization and Control Selection for National Security Systems**, October 2009, http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf

R. CJCSI 6211.02D, **Defense Information Systems Network (DISN) Responsibilities**, 24 January 2012
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf

APPENDIX C

Cloud-related Terms

Cloud Computing

As defined by NIST, cloud computing is a model for ena**bling ubiquitous, convenient, on-demand network access to a shared pool of configurab**le computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing services can be described by their shared characteristics, by the computing resources provided as a service, and by the method of deployment.

Cloud Models

> **Private Cloud**: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
>
> **Public Cloud**: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
>
> **Community Cloud**: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
>
> **Hybrid Cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models

- **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are

accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Cloud Service Characteristics

On Demand Self Service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource Pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid Elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and be rapidly released to quickly scale in.

Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Additional Cloud Terminology

Data as a Service (DaaS): "DaaS is based on the concept that the product, data in this case, can be provided on demand to the user regardless of geographic or organizational separation of provider and consumer. Additionally, the emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant. This development has enabled the recent emergence of the relatively new concept of DaaS." ***Wikipedia***

Virtualized Infrastructure: "Today's x86 computer hardware was designed to run a single operating system and a single application, leaving most machines vastly underutilized. Virtualization lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer." ***VMware***

Cross Domain Solution: A means of information assurance that provides the ability to manually or automatically access or transfer between two or more differing security domains. They are integrated systems of hardware and software that enable transfer of information among incompatible security domains or levels of classification. Modern military, intelligence, and law enforcement operations critically depend on timely sharing of information" ***Wikipedia***

Key Cloud Computing Roles

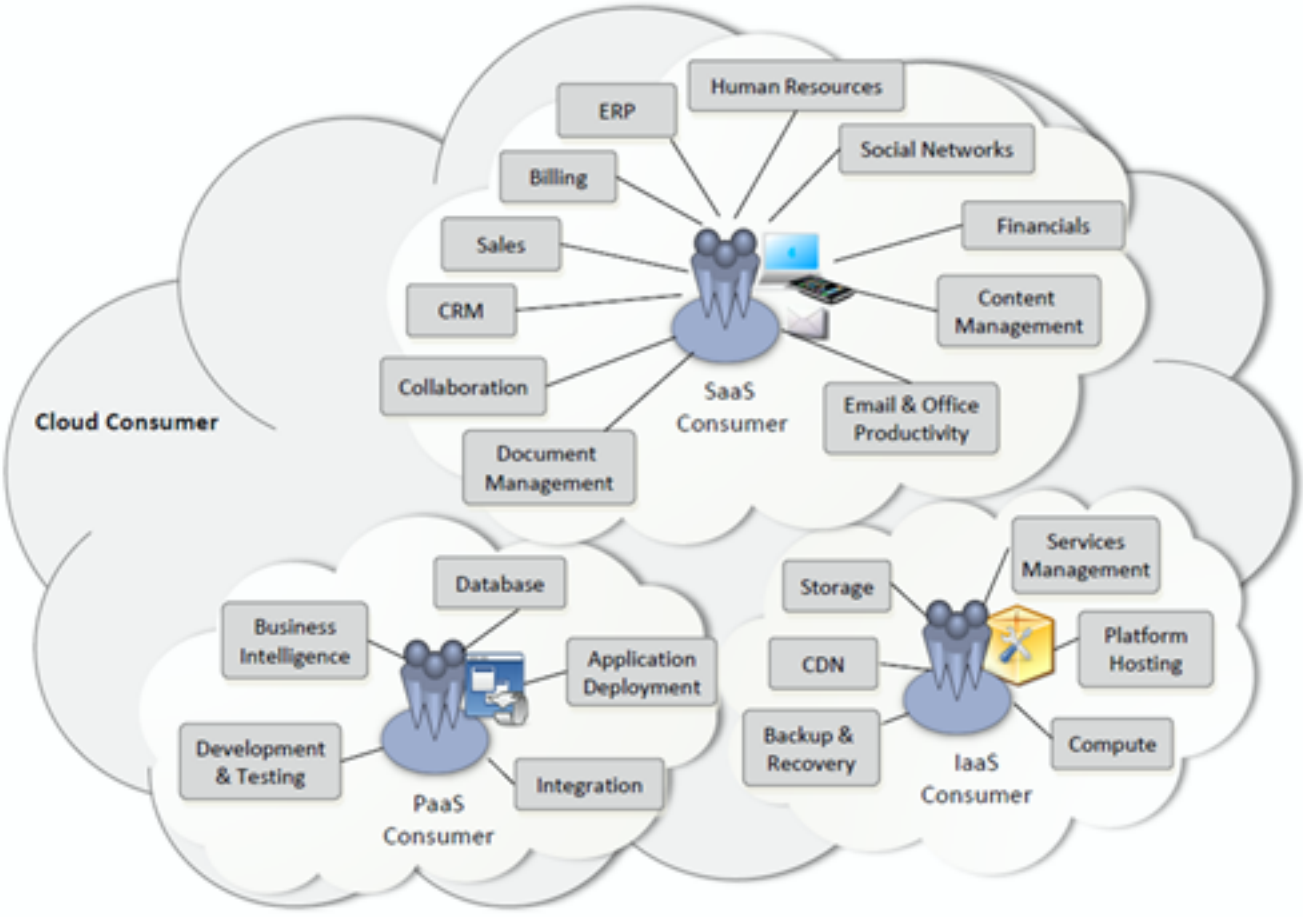
Service Consumer: Organization that decides to move certain IT resources from the confines of their enterprise to one or more external partners allowing them to focus resources on mission critical needs

Service Provider: Organization that decides to specialize in offering an IT service to multiple consumers over the net. The service provider invests in transitioning a traditional IT capability into a cloud service by implementing a massively scalable and dependable infrastructure, enabling customer self-service and metered use through

automation, ensuing ongoing service maintenance and continuous improvement, and providing exceptional customer support.

Cloud Products or Technology: Rather than providing a service that is consumed over a network, many of the cloud vendors provide products that enable their consumers to provide or consume cloud services.

Cloud Broker: A cloud broker is an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.



Example Services Available to Cloud Consumers, *NIST Cloud Computing Reference Architecture Draft*

Figure 3: Example Services Available to Cloud Consumers