25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT

Vivek Kundra

U.S. Chief Information Officer

DECEMBER 9, 2010

THE WHITE HOUSE
WASHINGTON

- Work with Congress to:
  - Consolidate commodity IT funding under the Agency CIOs and
  - Develop flexible budget models that align with modular development
- Launch an interactive platform for pre-RFP agency-industry collaboration

This plan is divided into two sections: Achieving Operational Efficiency and Managing Large-Scale IT Programs Effectively. The first section outlines the steps being taken to adopt cloud solutions and leverage shared services. The second section covers the structural areas that impact the success rates of large IT programs across government. The 25 action items listed throughout the plan are summarized in the chart at the end of the document.

PART I: ACHIEVING OPERATIONAL EFFICIENCY

As part of a broader IT transformation, the Federal Government needs to fundamentally shift its mindset from building custom systems to adopting light technologies and shared solutions. Too often, agencies build large standalone systems from scratch, segregated from other systems. These systems often duplicate others already within the Federal Government, wasting taxpayer dollars. The growth in data centers from 432 in 1998 to 2,094 in 2010 highlights this problem.

Leading private sector companies have taken great strides to improve their operating efficiencies. Cloud technologies and Infrastructure-as-a-Service enable IT services to efficiently share demand across infrastructure assets, reducing the overall reserve capacity across the enterprise. Additionally, leveraging shared services of "commodity" applications such as e-mail across functional organizations allows organizations to redirect management attention and resources towards value-added activities. The massive scale of the Federal Government allows for great potential to leverage these efficiencies.

The following section outlines actionable, achievable steps to improve the government's operational efficiency.

A. Apply "Light Technology" and Shared Solutions

The shift to "light technologies," that is, cloud services, which can be deployed rapidly, and shared solutions will result in substantial cost savings, allowing agencies to optimize spending, and allowing agencies to reinvest in their most critical mission needs. For example, GSA recently entered into a contract to shift email services to the cloud, resulting in a 50% cost reduction over five years – a savings of about $15 million. Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth by implementing a "Cloud First" policy for services, and increasing their use of available cloud and shared services.

1. Complete detailed implementation plans to consolidate at least 800 data centers by 2015

In February 2010, the Administration launched the Federal Data Center Consolidation Initiative (FDCCI) and issued guidance for Federal CIO Council agencies. The guidance called for agencies to inventory their data center assets, develop consolidation plans throughout fiscal year 2010, and integrate those plans into agency fiscal year 2012 budget submissions.

The FDCCI is aimed at assisting agencies in identifying their existing data center assets and formulating detailed consolidation plans that include a technical roadmap and clear consolidation targets. The FDCCI will cut down the number of data centers across the government and assist agencies in applying best practices from the public and private sector, with goals to:

- Promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers
- Reduce the cost of data center hardware, software, and operations
- Increase the overall IT security posture of the government, and
- Shift IT investments to more efficient computing platforms and technologies.

After an 8 month peer review process, we now know that the government is operating and maintaining almost 2,100 data centers. Through the FDCCI, a minimum of 800 data centers will be closed by 2015.

To meet this reduction target, OMB and Agency CIOs will take the following steps:

1.1 Identify agency data center program managers to lead consolidation efforts

Large IT projects often fail to meet goals because of distributed accountability for success. Large, complex, and critical infrastructure programs, such as data center consolidation, require a single person to lead the coordinated effort.

Within the next six months, each agency will designate a senior, dedicated data center consolidation program manager with project management experience and technical competence in IT infrastructure. Because data center consolidation requires interactions with many stakeholder groups, the data center

program manager must also have strong communication skills. The data center program manager at each agency will be responsible for developing a plan with interim, verifiable milestones to reach the agency's data center reduction target and monitor progress toward those goals.

1.2 Launch a Data Center Consolidation Task Force to ensure successful execution

Within the next three months, the Federal CIO Council will launch a government-wide Data Center Consolidation Task Force comprised of the data center program managers, facilities managers, and sustainability officers. The Data Center Consolidation Task Force will be responsible for working together to share progress toward individual agency goals and the overall Federal target of a minimum of 800 data center closures by 2015. The Data Center Consolidation Task Force will meet monthly to review progress of each consolidation project and ensure government-wide alignment between agency efforts where appropriate. The Task Force will serve as a "community of practice" for Agency CIOs and data center program managers to share best practices from this effort and enhance consolidation effectiveness.

1.3 Launch a publicly available dashboard to track data center consolidation progress

OMB will launch a publicly available dashboard to serve as a window into progress of the data center consolidation program. The dashboard will ensure transparency and accountability, and keep the overall program in plain view of the public.

2. Create a government-wide marketplace for data center availability

Within the next 18 months, OMB and GSA will create a government-wide marketplace that better utilizes spare capacity within operational data centers.

This online marketplace will match agencies with extra capacity to agencies with increasing demand, thereby improving the utilization of existing facilities. The marketplace will help agencies with available capacity promote their available data center space. Once agencies have a clear sense of the existing capacity landscape, they can make more informed consolidation decisions.

3. Shift to a "Cloud First" policy

In the private sector, a web-based multimedia production company used the cloud to allow anyone with access to an Internet connection the ability to create their own fully customized, professional-quality, TV-like videos. Consumers can then share the resulting videos with friends and family across the world. The cloud allowed for a rapid response when demand jumped from 25,000 users to more than 250,000 users in three days, eventually reaching a peak rate of 20,000 new customers every hour. Because of the cloud, the company was able to scale from 50 to 4,000 virtual machines in three days to support increased demand on a real-time basis.

In contrast, the Federal Government's Car Allowance and Rebate System (CARS, more commonly known as "Cash-For-Clunkers") failed when faced with peak loads. To process the anticipated 250,000 transactions, the National Highway Traffic Safety Administration (NHTSA) deployed a customized commercial application hosted in a traditional data center environment on June 19, 2009. When dealer registrations

began on July 24, 2009, demand far exceeded initial projections, and within three days, the system was overwhelmed, leading to numerous unplanned outages and service disruptions. Ultimately, approximately 690,000 CARS transactions were processed. However, lacking the ability to scale rapidly, system stability was not achieved until August 28, 2009, over a month after registrations started coming in.

The Federal Government must be better prepared in the future. Beginning immediately, the Federal Government will shift to a "Cloud First" policy.

The three-part strategy on cloud technology will revolve around using commercial cloud technologies where feasible, launching private government clouds, and utilizing regional clouds with state and local governments where appropriate.

Cloud computing brings a wide range of benefits:

- *Economical*: Cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required to begin, and additional investment is needed only as system use increases.
- *Flexible*: IT departments that anticipate fluctuations in user demand no longer need to scramble for additional hardware and software. With cloud computing, they can add or subtract capacity quickly and easily.
- *Fast*: Cloud computing eliminates long procurement and certification processes, while providing a near-limitless selection of services.

When evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. To facilitate this shift, we will be standing up secure government-wide cloud computing platforms.

3.1 Publish cloud strategy

Within the next six months, the Federal CIO will publish a strategy to accelerate the safe and secure adoption of cloud computing across the government.

The National Institute of Standards and Technology (NIST) will facilitate and lead the development of standards for security, interoperability, and portability. NIST is working with other agencies, industry, academia, standards development organizations, and others to use existing standards as appropriate and develop cloud computing standards where gaps exist. While cloud computing services are currently being used, experts cite security, interoperability, and portability as major barriers to further adoption. The expectation is that standards will shorten the adoption cycle, enabling cost savings and an increased ability to quickly create and deploy enterprise applications.

3.2 Jump-start the migration to cloud technologies

Each Agency CIO will be required to identify three "must move" services and create a project plan for migrating each of them to cloud solutions and retiring the associated legacy systems. Of the three, at least one of the services must fully migrate to a cloud solution within 12 months and the remaining two within 18 months.

Each migration plan will include major milestones, execution risks, adoption targets, and required resources, as well as a retirement plan for legacy services once cloud services are online. These new cloud implementations should be compatible with the secure, certified platforms currently provided in the private sector. Migrating these services will build capabilities and momentum in the Federal Government, encourage industry to more rapidly develop appropriate cloud solutions for government, and reduce operating costs.

4. Stand-up contract vehicles for secure IaaS solutions

Federal, state, and local governments will soon have access to cloud-based Infrastructure-as-a-Service (IaaS) offerings. GSA's IaaS contract award allows 12 vendors to provide government entities with cloud storage, virtual machines, and web hosting services to support a continued expansion of governments' IT capabilities into cloud computing environments.

Within the next six months, after completing security certification, GSA will make a common set of contract vehicles for cloud-based Infrastructure-as-a-Service solutions available government-wide.

A government-wide risk and authorization program for cloud computing will allow agencies to rely on the authorization completed by another agency or to use an existing authorization, so that only additional, agency-specific requirements need to be separately certified. Our aim is to drive to a set of common services across the government supported by a community, rather than an agency-specific risk model. This will allow the Federal Government to "approve once and use often."

5. Stand-up contract vehicles for commodity services

The Software-as-a-Service (SaaS) E-mail Working Group, formed in June 2010, has begun to identify and develop the set of baseline functional and technical requirements for government-wide cloud email solutions and is working towards developing business case templates for agencies who are considering transitioning to SaaS e-mail.

Within 12 months, GSA will utilize these requirements to stand up government-wide contract vehicles for cloud-based email solutions. GSA will also begin a similar process specifically designed for other back-end, cloud-based solutions.

6. Develop a strategy for shared services

Within the next 12 months, the Federal CIO will develop a strategy for shared services. That strategy will build on earlier Federal Government successes in shared services and include benchmarks on current usage and uptake rates, as well as service level agreements (SLAs), customer satisfaction levels, costs, and overall economic effectiveness.

Managing partners of shared services will assess the current state of shared services and each release a roadmap to improve quality and uptake. Ultimately, the managing partners will be responsible for executing these roadmaps and will be held accountable for improvements on SLAs and reductions in cost. These efforts will enable the current shared services to be accessible government-wide at higher quality levels.

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

DEC 15 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services

References: (a) DoD Memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012 (Canceled)
(b) DoD Memorandum, "Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services," December 16, 2013 (Canceled)
(c) DoD Memorandum, "Use of Enterprise Information Technology Standard Business Case Analysis," October 23, 2014
(d) Federal Risk Authorization and Management Program, http://cloud.cio.gov/fedramp
(e) DoD Instruction 8500.01 "Cybersecurity", March 14, 2014

This memo clarifies and updates DoD guidance when acquiring commercial cloud services, and hereby cancels and replaces references (a) and (b). In the context of this memo, commercial cloud services also refer to cloud services provided by Non-DoD federal government organizations.

1. DoD components may acquire cloud services directly. It is no longer a requirement to use DISA for the acquisition of cloud computing services.

2. Each Component remains responsible for determining what data and missions are hosted by external cloud service providers per the direction below.

3. Each use of cloud services must be analyzed using the Enterprise IT Business Case Analysis (BCA) template as provided in reference (c). The BCA must be approved by

the Component CIO and a copy submitted to the DoD CIO. DISA provided cloud services must be considered as part of the BCA.

4. The Federal Risk Authorization and Management Program (FedRAMP) will serve as the minimum security baseline for all DoD cloud services as described in reference (d). Per current policy, components may host Unclassified DoD information that has been publicly released on FedRAMP approved cloud services.

5. For more sensitive DoD unclassified data or missions (called *Sensitive Data* below), DoD has developed cloud security requirements and guidance that go beyond FedRAMP. A draft of this *DoD Cloud Computing Security Requirements Guide* (the Guide) is currently out for DoD public comment, with official release scheduled for January 7, 2015. The Guide is intended to give cloud providers a stable security requirement, and to help DoD cloud customers move more rapidly and securely into the cloud. The Guide defines several classes of Sensitive Data, with increasing security requirements for each. Additional detail on the Guide and the Guide development process can be found in paragraph 11.

6. Any cloud service provider that is interested in hosting Sensitive Data will submit evidence to DISA that the provider meets specific requirements of the Guide. DISA will evaluate this evidence and if the provider meets the requirements, DISA will issue a DoD Provisional Authorization (PA). The PA will describe the types of information and mission that can be hosted by a particular cloud service.

7. Per the BCA of paragraph three, using the customer guidance in the Guide and the information in the PA, the CIO of each Component will determine which cloud service provider to use for a particular set of information or mission. DoD Components may only host Sensitive Data in cloud service providers that have an appropriate PA.

8. Commercial cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point (CAP) provided by DISA or through a CAP provided by another DoD Component. All CAPs must be approved by DoD CIO. The current Navy CAP is an example of an approved provisional cloud access point. In the future, in order to standardize cyber defenses, our goal is that all DoD access to commercial cloud services be via a DISA provided CAP. This CAP will protect all DoD missions from incidents that affect a particular cloud service provider, and will provide perimeter defenses and sensing for applications hosted in the commercial cloud service.

9. Operations in a cloud environment are diverse and will require different concepts of operations (CONOPS), business strategies, etc. Components are responsible for cyberspace defense of all information and missions hosted in commercial cloud services, and will share cyberspace defense information as necessary and appropriate with cloud service providers, in accordance with reference (e). DoD Components that acquire or use cloud services are still responsible for ensuring that end to end security requirements are met. To operate and defend successfully, this will require collaboration and information sharing among the Component, DISA and the cloud service provider.

10. The *DoD Cloud Computing Security Requirements Guide* will be an evolving document informed by public and private input. It is intended to be a collaborative document between the government and private sector that recognizes the rapid technology and business changes in the cloud services environment. To assist in the development and use of the *DoD Cloud Computing Security Requirements Guide*, DoD will be holding a series of meetings, the first being a technical interchange meeting in person and via the web with interested DoD and industry partners on December 18, 2014. Comments on the draft *DoD Cloud Computing Security Requirements Guide* are due by December 29, 2014. Details can be found at http://iase.disa.mil/cloud_security/Pages/index.aspx. In January 2015, the Deputy CIO for Cybersecurity will host the first regular meeting with DoD and industry, at which time the organizations with key cloud responsibilities in DoD will describe DoD requirements, processes, and plans, and seek feedback from our government, private and public partners in the cloud environment. In addition, comments on the Guide are welcome at any time, via the following email address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

11. Additional information on procuring cloud services is provided in attachment (1).

DoD CIO point of contact for cloud is Robert Vietmeyer, robert.w.vietmeyer.civ@mail.mil, (571) 372-4461. The DISA point of contact is the Risk Management Office, disa.meade.ma.mbx.maops@mail.mil, (301) 225-7900.

Terry A. Halvorsen
Acting

Attachment:
As stated

ATTACHMENT 1

CLOUD SERVICE PROCUREMENT INFORMATION

DoD Components are responsible for acquiring the Information Technology (IT) services that meet their mission objectives and provide an optimal solution compliant with DoD cybersecurity requirements. Components will:

1. Address the contractual risks and issues associated with cloud services identified in the DoD Cloud Computing Issues matrix in all contracting vehicles that are used to acquire commercial cloud services, found at https://dodcioext.osd.mil/SitePages/Cloud_Computing.aspx. Defense Procurement and Acquisition Policy will develop appropriate contract language to address the issues, guidance and requirements in DFARS Case 2013-D024, Contracting for Cloud Services.

2. Register use of the Cloud Service Provider (CSP) in the DoD Information Technology Portfolio Registry (DITPR) and report its use as part of the Components Federal Information Security Management Act (FISMA) report.

3. Report all appropriate information within the Select and Native Programming Data Input System – Information Technology (SNaP-IT) as directed in DoD CIO annual IT budget guidance for each utilized cloud computing service.

4. Request exceptions to these requirements for commercial cloud services using the DoD Information Networks (DODIN) Waiver Process.

5. Track the evolution and use the latest versions of the references and any published concepts of operation in all new cloud deployments. Cloud services, DoD programmatic approaches to cloud services, technical approaches for connecting to cloud services, and operational approaches for defending DoD information and missions hosted in cloud services are all evolving continuously. To ensure dependable mission execution and information security, Components will use the most recent guidance, requirements and policies to support their cloud deployments.

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cloud Computing Strategy

The Department is committed to realizing the value of cloud computing and providing a secure enterprise cloud environment, in alignment with Federal and Department-wide IT efficiency initiatives. The federal government intends to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to "evaluate safe, secure cloud computing options before making any new IT investments." The attached DoD Cloud Computing Strategy lays the groundwork, consistent with the Federal Cloud Computing Strategy, for accelerating cloud adoption in the Department. The strategy includes steps to foster adoption of cloud computing, optimize data center consolidation, establish the DoD enterprise cloud infrastructure and continue to deliver cloud services. A robust and resilient multi-provider, Enterprise Cloud Environment will enable the Department to achieve the goals of the Joint Information Environment.

An implementation plan will follow, which will include further detail. In addition, a communications plan will promote the "Enterprise-first" approach to cloud computing and the use of a DoD Enterprise Cloud Services Broker, and address the cultural challenges associated with the adoption and implementation of cloud services. The existing Cloud Computing Working Group, led by the DoD CIO and the Defense Information Systems Agency, will continue to support follow-on strategy efforts.

The DoD CIO point of contact for DoD Cloud Computing is Mr. Robert Vietmeyer at email: robert.vietmeyer@osd.mil, 571-372-4461.

Teresa M. Takai

Attachment:
As stated

Department of Defense

Chief Information Officer

Cloud Computing Strategy

July 2012

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.

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

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

1.3 Audience

The intended audience of this document is system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

2. The NIST Definition of Cloud Computing

Cloud computing is 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. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models.

Essential 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 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, tablets, laptops, and workstations).

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 datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] 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.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. 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

[1] Typically this is done on a pay-per-use or charge-per-use basis.

[2] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

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).

Deployment 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.

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.

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.

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).

[3] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.