# Federal Data Center Consolidation Initiative

# Department of Defense
# 2011 Data Center Consolidation Plan
# &
# Progress Report
## *November 8, 2011*


1 Introduction ..... 2
2 Agency Goals for Data Center Consolidation ..... 2
3 Implementing Shared Services/Multi-tenancy ..... 4
4 Agency Approach, Rationale and Timeline ..... 6
5 Agency Governance Framework for Data Center Consolidation ..... 8
DoD CIO Executive Board ..... 9
Enterprise Guidance Board ..... 9
DoD Data Center Consolidation Working Group ..... 9
5.1 Cost-benefit Analysis ..... 9
5.2 Risk Management and Mitigation ..... 10
5.3 Acquisition Management ..... 11
5.4 Communications Strategy ..... 12
6 Progress ..... 13
6.1 FDCCI Consolidation Progress ..... 13
6.2 Cost Savings ..... 14

# 1 Introduction

The Department of Defense (DoD) has made great strides over the last decade in consolidating data centers and IT infrastructure by focusing on Base Realignment and Closure Act (BRAC) consolidation, Component consolidation efforts, and optimization of the Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs). Most DoD Components and Defense Agencies have planned or begun to consolidate data centers, virtualize servers and leverage cloud computing, in part, to respond to downward pressure on Federal agency spending that will continue to intensify as part of deficit reduction efforts. 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 described in the DoD Information Technology (IT) Enterprise Strategy and Roadmap (ITESR). The purpose of consolidation is to optimize DoD computing centers and establish Core data centers to support critical enterprise services. These efforts are consistent with the Federal Data Center Consolidation Initiative (FDCCI) that seeks to reverse the historic growth of Federal data centers. The Department remains committed to supporting this initiative.

DoD and its Combatant Commands/Services/Agencies (CC/S/As) are considering all options for achieving consolidation that includes migrating infrastructure to Defense Information Systems Agency (DISA) enterprise computing centers (DECCs), valid commercial options to reduce costs of IT services, cross-Component co-hosting, virtualization/cloud computing, to name a few. As examples, the Air Force, Army and the Defense Logistics Agency (DLA) have adopted a “DISA First” strategy for data center consolidation. With the “DISA First” strategy, they will consider DISA for application and data hosting before pursuing any other solutions.

DoD required all consolidation plans to be submitted with a signed verification letter from agency CIOs attesting to the accuracy and completion of information. The Department is participating in an inter-agency peer review process.

# 2 Agency Goals for Data Center Consolidation

DoD’s strategic objectives for data center consolidation include:

- Reduce cost
- Reduce environmental impact

- Improve efficiency and service levels via automation
- Enhance business agility and effectively manage change

Specifically, goals include:

- Reducing the Total Cost of Ownership (TCO) for local data center hardware, software and operations by hosting and managing applications in DISA-managed DOD Enterprise Computing Centers
- Procuring application hosting and IT services from DISA which reduces the need for local contractor support and services. (Commercial and/or local data centers may be considered when centralizing in DISA is not practical)
  - Hosting Enterprise Applications within DISA DECCs will shift IT operations focus from infrastructure management to service management model outlined in Federal Cloud Computing strategy
  - Reducing the overall energy and real estate footprint at primary level field activities as a result of application consolidations into DISA DECCs
- Implementing better standardization, automation and continuous risk monitoring by hosting applications in secure Core data centers
- Highlights of Components goals are provided below:
  - The Army's Data Center Consolidation Plan (ADCCP) defines an initial goal to close 185 of its data centers by the end of FY15, with further reductions to be considered thereafter. The ADCCP establishes standards and assigns responsibility for the rationalization and migration of applications software and consolidation of data centers. The effort will consolidate data centers and applications, provide enterprise hosting as a managed service, and improve the security of Army information assets. Through consolidation, the Army expects to reduce significantly its inventory of data centers; improve the efficiency of operations and services; improve the security of computer and information assets; and achieve centralized hosting of services while transitioning to standardized computing environments. Closing Army data centers will require the purchase of enterprise hosting as a managed service, with a long-term goal of decreasing the Army's IT infrastructure and application inventory. The Army will maintain a limited number of data centers to support local installation services only as required; these data centers will be the exception
  - Results from an empirical analysis of the data gathered reflect a 47% reduction of Air Force data centers by FY15
  - The Navy seeks to achieve a reduction of more than 50% data centers by FY15. The Navy plans to virtualize applications, consolidate servers and reduce the number of data centers supporting the Navy Enterprise

- The Marine Corps will reduce costs and save manpower by achieving economies of scale by deploying enterprise services and applications on Marine Corps Enterprise Information Technology Services (MCEITS)
- DLA established an aggressive, but achievable goal of a minimum 75% reduction in the number of servers and 90% reduction in the number of DLA managed data centers. The 75% reduction in servers represents an estimate based on virtualization efforts as well as migration efforts to the DISA DECCs. DLA plans to close nearly all its data centers by the end of 2015
- The Military Health System target is to reduce the number of data centers by 70% over a 5-year time frame

The qualitative impacts include:

- Enhance Mission Effectiveness: Consolidating data centers and servers results in increased mission effectiveness for both the network community and functional users. Consolidation provides an opportunity to centralize management, streamline operations, and standardize on a more flexible architecture. This is beneficial during disaster recovery operations, maintenance, system outages, or resource utilization imbalances
- Improve Security: Data center and server consolidation also results in improved network, data, and physical security. Centralized data centers provide increased physical security for servers, and those with enterprise-class network security devices such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls provide enhanced network security. Hosting virtualized servers in pre-configured, standardized hosting enclaves also expedites the certification and accreditation (C&A) processes through inheritance
- Streamline IT Provisioning and Effectiveness: The ability of the Department to respond to changing mission needs depends on the speed of IT resource provisioning and reconfiguration. Data centers with non-standardized infrastructures and stove-piped architectures require more effort to operate and maintain. The process of developing and delivering new capabilities will be expedited as a result of standardized provisioning.

# 3 Implementing Shared Services/Multi-tenancy

DoD relies on DISA as its shared hosting provider, offering computing services to the entire DoD community from within shared/multi-tenant Defense Enterprise Computing Centers (DECC) and other venues. DISA offers hosting and information processing capabilities as well as Net-Centric Enterprise Services (NCES), which provide connections between people and systems to enable

the sharing of data and services. Under the Defense Information Systems Network (DISN), DISA provides voice, video, and data in addition to technical support services.

The DoD ITESR Near Term Plan represents DoD CIO guidance, focused on an initial set of eight initiatives to drive realization of the goals put forth in the ITESR. These initiatives are the first steps of a substantial effort that includes twenty six initiatives. Six of these eight near-term initiatives are described below (the other two are described in Section 5.3):

- Consolidate Security Infrastructure - Establish a boundary protection structure that identifies a complementary set of information assurance protection mechanisms. The IT consolidation efforts will evolve and improve the security architecture of the Non-secure Internet Protocol Router Network (NIPRNet), and ultimately the Secure Internet Protocol Router Network (SIPRNet).

- Implement Cross-Domain Solution as an Enterprise Service – Deploy a comprehensive, enterprise-level cross-domain service. To the greatest extent practicable cross-domain solutions should be hosted at the enterprise level, administered in accordance with DoD CIO policy, and under the oversight and direction of USCYBERCOM in order to strengthen cyber security as well as curb escalating costs.

- Joint Information Environment (JIE)/Joint Enterprise Network (JEN) – Deploy the JEN to maximize utilization of DoD IT investments in a given region without compromising security. DoD is developing the Global Information Grid (GIG) 2.0 as a single coherent, secure, and consolidated information environment that represents a fundamental shift in how we design, implement, manage, operate, and maintain DoD information technology at all levels. GIG 2.0 will transform the multiple intranets that comprise today's GIG to a single information environment. The GIG 2.0 provides a vision of a single, secure information environment which will be realized through the Joint Information Environment (JIE).

- Data Center and Server Consolidation - Optimize DoD computing centers and establish Core data centers to support critical enterprise services. This consolidation of data centers is expected to yield significant cost savings to the Department. In addition, DoD will establish a federation of standardized Core data centers involving key data centers from DISA, Army, Air Force, and the Department of the Navy that will support critical enterprise services. The footprint and connectivity of the data centers will have a global reach making their services accessible from anywhere necessary to support mission execution.

- Enterprise Messaging and Collaboration (including Email) – Facilitate DoD-wide communication and collaboration through an enterprise-level solution. Provide a set of Enterprise Messaging and Collaboration capabilities, to include IM/Chat, Email, Portal, and

Web conferencing, that enable information sharing from any device attached to a DoD network. This initiative also involves integrating these capabilities with others that are being acquired (e.g., Voice and Video) as defined in the Unified Communications and Collaboration strategy. These services will be location independent, allowing deployed forces to seamlessly disconnect from the home station and reconnect to communication and collaboration services at forward locations without the need for intensive manual administrative processes.

- Identity and Access Management (IdAM) Services - Establish an enterprise-level infrastructure to allow access to required resources through standardized credentialing. The Department will define and implement enterprise-wide IdAM services that are based upon consistent access control decisions which can be traced back to policy, regulation, and law. The DoD-level approach for IdAM is a critical enabler for secure net-centric information sharing. The consistent implementation of the core IdAM services of identity, authentication, and dynamic access control will materially improve the flexibility and agility of the warfighter.

# 4 Agency Approach, Rationale and Timeline

DoD's approach for consolidation consists of increasing reliance on Core data centers to support critical enterprise services and reducing Component data centers. The DoD goal is to establish Core, regional, installation, and deployable data centers that will meet minimum standards to support enterprise applications/services. The Core data centers will gradually absorb many of the applications/services currently hosted in numerous Component data centers, enabling the latter to be closed. DoD is developing the DoD Data Center and Server Consolidation Reference Architecture. This DoD-wide reference architecture is intended to guide Enterprise and C/S/A efforts for consolidating and optimizing data centers to achieve Department goals as part of the ITESR. These goals include increased mission effectiveness, increased security and enterprise-wide efficiencies utilizing Green IT practices. By focusing on these goals and leveraging cloud computing capabilities, the Department will define its future computing infrastructure in order to move toward a more secure, sustainable, services-based Information Enterprise (IE) that ensures mission effectiveness at both the enterprise level and the tactical edge.

To achieve these goals, DoD will focus on two key elements that will assist in the establishment of the Core: Capability Design and Development and Program Management/Stewardship.

- **Capability Design and Development:**

  This effort includes:

  - The issuance of new DoD policy (DoD Instruction 8440.bb, currently draft) and guidance that clearly define the standards and attributes of the Core data centers

- A reference architecture for the Core intended to establish technical, system, and operational relationships among Core data centers
- Implementation plans that direct the fielding of the Core architecture.
- Component data center consolidation plans
- A moratorium on establishing new data centers
- Service Level Agreements

- **Program Management/Stewardship:**

  This effort includes:

  - Establishment of the DoD CIO, with the support of DoD CIO Executive Board, as the final decision authority for developing and sustaining the Core as executed by the Components
  - Appointment of a DoD Data Center Consolidation Working Group that will oversee Component progress in data center consolidation and orchestrate coordination across organizational boundaries
  - Consolidation of data centers by DoD CC/S/A's which will be overseen by DoD CIO. This oversight includes reviewing CC/S/As asset inventories, consolidation plans and progress reports. CC/S/As will develop their own individual consolidation schedules that are appropriate for their organization
  - DoD CIO will conduct a business case analysis to support infusion of funding to establish the Core and a follow-on effort to establish a funding model to sustain the Core

DoD Components are developing consolidation plans to reduce their data center inventory. Many of these plans consist of a short-term strategy that focuses on pre-existing and ongoing IT consolidation and efficiency initiatives that can deliver early successes, and a long-term 'DISA First' strategy. Examples of DoD Components that are adopting a 'DISA First' strategy are the Air Force, the Army and Defense Logistics Agency.

Several examples of Components' approaches for consolidation are provided below:

The Army will use the Application Migration Concept of Operations as a guide to consolidate and migrate applications from its current local and functional data centers to DoD enterprise data centers. In addition, a Memorandum issued by the Secretary of the Army on 9 September 2011 directs that the Army's 2010 moratorium on the procurement of all servers will be expanded to include a moratorium on the construction and/or renovation of Army data centers and server rooms. In particular, the SecArmy Memorandum prohibits the procurement of servers and the construction or renovation of hosting facilities without a written waiver, granted in advance by the Headquarters, Department of the Army (HQDA), CIO/G-6, consistent with the HQDA Army Data Center Consolidation Plan Execution Order, which was published on 9 May 2011.

The Air Force's short-term strategy includes the following:

***Air Force Network (AFNet) Migration*:** A major objective of the AFNet Migration program is to collapse the multiple major command (MAJCOM)-centric Active Directory (AD) and Microsoft

Exchange architectures into a single consolidated, centrally managed Air Force enterprise architecture. This provides decision makers with unmatched situational awareness and command and control (C2) of network forces.

***Air National Guard (ANG) Network Control Center Rebuild (NCC-R)*:** The NCC-R initiative is deploying a consolidated and standardized virtual infrastructure platform to all of the ANG data centers. This will result in significant reduction in physical server counts, floor space, cooling requirements, and power costs. The ANG plans to reduce 48 more data centers through this initiative in FY12.

***Air Force IT Efficiencies Objective Two – 'Consolidate Network IT':*** This effort seeks to reduce the number of Air Force servers through virtualization and will consolidate nine MAJCOM and regional processing centers (RPC) into five centralized enterprise APCs. Furthermore, this initiative will prepare the Air Force for further consolidation into enterprise computing facilities as recommended by DISA.

***Additional Consolidation Candidates:*** The Air Force MAJCOMs, excluding the ANG, identified a total of 32 data centers that could be closed between FY12-15.

DLA's approach consists of several elements:

- Virtualize existing applications to the largest extent
- Migrating applications to DISA DECCs
- Consolidate DLA Test and Development Environments
- Establish Application Development Standards

The Military Health System (MHS) is considering the following options as part of its efforts to reduce infrastructure: decommissioning, site centralization, server/storage virtualization, virtualization, and cloud computing. MHS' implementation plans seek to achieve a reduction of 50% or more (the target is 70%) data centers.

The Defense Personnel Security Research Center's (PERSEREC) approach to the consolidation effort was and continues to be to first identify the best physical and functional candidates for consolidation, repurpose and reconfigure IT resources to best support the mission and introduce standardization within hardware, platform and application design and management.

The Defense Commissary Agency's (DeCA) approach to the virtualization effort is multifaceted; one part is to virtualize the current operating environment, the other is to upgrade and streamline current systems to accommodate the more technologically advanced virtual environment. DeCA want to reduce the energy consumption foot print, and also reduce server management, contract support and provisioning through improved automation. This goal requires complete system refreshes for some, while other systems merely need some code modifications.

# 5 Agency Governance Framework for Data Center Consolidation

The standard DoD governance structure will be used to manage the Department's data center consolidation efforts. This framework is as follows:

## DoD CIO Executive Board

The primary mission of the Executive Board is to advance the DoD's goals in the areas of information management, information interoperability and information assurance between and among Defense components. The DoD CIO Executive Board is the principal DoD forum to advise the DoD CIO on a full range of matters pertaining to the Global Information Grid (GIG) and the Information Enterprise.

## Enterprise Guidance Board

The DoD CIO Enterprise Guidance Board (EGB) is tasked by the DoD CIO, as a subordinate board to the DoD Chief Information Officer Executive Board (DoD CIO ExBd) to perform five major functions for the department:

- Review DoD CIO enterprise-wide architecture, strategies and policies to determine effectiveness and deficiencies, with resulting courses of action, in satisfying DoD mission needs.
- Develop and publish strategies, guidance and tool requirements to support the analysis and management of IT across the Department to include the DoD Capability Portfolios Managers (CPMs), Component CIOs, and Component Acquisition Executives (CAEs).
- Provide guidance to the Department on the evolution of the Federated DoD Enterprise Architecture.
- Guide the development of, and ensure compliance with, the DoD Information Enterprise Architecture (IEA) and related policies.
- Serve as the Senior Steering Group (SSG) for the Corporate Management and Support (CM&S) Tier II Information Management JCA.

The DoD CIO EGB assists the DoD CIO develop and implement enterprise level guidance for IT Infrastructure optimization, which is incorporated into the core business processes of Department (i.e. requirements validation, budgeting and acquisition). Individual DoD Components have component level governance structures to review, plan, execute and monitor IT investments internally.

## DoD Data Center Consolidation Working Group

The DoD Data Center Consolidation Working Group (DCCWG) has representation from all DoD CC/S/As. The working group vets and develops approaches to achieve consolidation. The purpose of DCCWG is to reverse the historic growth of DoD data centers. The overall scope of the DCCWG is to serve as the central group for Departmental collaboration and coordination - guiding, identifying, and disseminating critical of information, solutions and processes that will help data center consolidation.

## 5.1 Cost-benefit Analysis

DoD Components are at varying stages of completing Business Case Analysis (BCA) given the size and complexity of DoD. Examples are described below:

The Department of Navy CIO established an integrated project team (IPT) to develop resources to assist in the execution of data center consolidation. The IPT created a data center requirements documentation tool and a BCA template to be completed for each data center or part of a data center that will be part of the migration and consolidation. These tools will assist the Navy in providing the technical assessment and cost estimation for migrating resources.

While the Navy has established a notional plan for migrating and closing the majority of non-NMCI data centers, the technical authority for Navy, the Space and Naval Warfare Systems Command (SPAWAR), has not completed full technical assessment of the consolidation plan. The SPAWAR technical assessment will include an estimation of the cost to perform each migration as well as the estimated cost to sustain these resources in a Navy Enterprise Data Center. Once complete, a more detailed analysis of the costs, benefits, and savings will be performed, and the prioritization and scheduling of the consolidation efforts can be optimized.

The Air Force is developing a BCA that will use several rigorous methodologies to analyze cost and provide models to determine savings. The BCA is expected to be completed in early FY12. The BCA strategy is being adjusted to include the "DISA First" strategy. This effort entails inclusion of upfront must-pay costs and the longer term savings of infrastructure and management reduction to be realized by the Air Force.

The Defense Logistics Agency's (DLA) plan for cost-benefit analysis follows:

- Identify each application, including the hardware and software used.
- Identify all of the direct and indirect costs and support requirements for each application.
- Implementation of subordinate element POA&Ms.
- Obtain service quotations and migration support requirements from DISA.
- Prioritize application migration to the DISA DECCs.

## 5.2 Risk Management and Mitigation

The EGB and the DoD CIO Executive Board will regularly receive updates on data center consolidation progress and take corrective actions and implement an escalation strategy to manage risk.

Risk management and mitigation is overseen jointly by DoD Components and the DoD CIO through the existing DoD governance process. The DoD CIO is responsible for overseeing all DoD computing operations, programs, systems, and initiatives. The Heads of DoD Components are responsible for implementing, monitoring, optimizing, and controlling consolidated GIG fixed CI node operations based upon desired mission capabilities and technical requirements, enhanced operational effectiveness, and competitive best value or other cost efficiencies that do not adversely affect security, mission, and/or technical requirements.

DoD Components have adopted various risk management strategies. Essentially, these comprise of two steps (i) risk identification and prioritization, and (ii) risk management and mitigation. Risks are tracked at several levels to include:

- Schedule Risk – the likelihood the project will not be completed within the specified schedule. Alternatively, the planned project schedule is inadequate so as not to allow sufficient time for all required tasks to be completed within planned schedule.
- Project Resources Risk – the likelihood that necessary resources will not be available in time or that the required knowledge/skills will not be available when needed.
- Dependency and Interoperability Risk – addresses the environment in which the project is being developed and in which the system will operate. Dependency Risk is the likelihood that the implementing organization will not receive intended benefits from the project due to its dependency upon another organization or project for delivery of critical project elements or project risk control elements. Interoperability Risk is the likelihood that the intended solution will not interact well with other systems of the Agency or external organizations lack of familiarity with and completeness of the interfaces, and immaturity of the service exchange concept among different solutions.
- Life-Cycle Costs Risk – the likelihood that total acquisition, operation and maintenance, and retirement costs of a project may be higher than estimated, due to the difficulty involved in forecasting future events affecting the costs.
- Organization/Change Management Risk – the likelihood that the organizational/agency/ government-wide cultural resistance to change and standardization, tendency to bypass required organizational changes, lack of use or improper use or adherence to new systems and processes, and inadequate training planning will result in organizational friction, resulting in implementation difficulty.
- Technology Risk – the likelihood that the new development of the new solution or expansion of an existing one will fail to provide a greater level of performance than previously demonstrated, will fail to achieve an existing level of performance due to new constraints or will fail to operate as designed.

## 5.3 Acquisition Management

DoD leverages DoD-wide and government-wide acquisition vehicles, as well as those negotiated by individual Components. DoD Enterprise Software Initiative (ESI) is an official DoD initiative sponsored by the DoD Chief Information Officer (CIO) to save time and money on commercial software, IT hardware, and services. Through its joint team of experts, requirements are consolidated and agreements are established with IT providers resulting in a unified contracting and vendor management strategy across the entire department. In its first ten years of operation, DoD ESI achieved a cost avoidance of over $3 billion off prices established on the GSA Federal Supply Schedule. The DoD Enterprise Software Initiative (ESI) leads in the establishment and management of enterprise COTS IT agreements, assets, and policies for the purpose of lowering total cost of ownership across the DoD, Coast Guard and Intelligence communities. ESI establishes strategic sourcing relations with leading information technology vendors to produce

Enterprise Software Agreements (ESA) containing favorable pricing, terms and conditions for buyers. Close working relations exist with the Intelligence Community, and with OMB/GSA SmartBUY Program.

Specifically, DoD will implement the following two initiatives as part of the DoD ITESR Near Term Plan:

- Consolidate Software Purchasing - In order to address the rising costs of DoD IT and the lack of interoperability that results from uncoordinated IT investments, the Department must consolidate, to the greatest extent practicable, contracts for the procurement of software solutions. This will allow the Department to leverage aggregate department buying power and achieve increased efficiency by securing more favorable contract terms. Further, fewer contracts will require less overhead support, thus generating additional cost avoidance.

  - This initiative involves centrally funding and managing DoD-wide enterprise licenses for the most widely used commercial software through the DoD ESI. DoD ESI will consolidate existing major Component-level enterprise licenses, or establish new DoD enterprise licenses, by negotiating advantageous pricing, terms, and conditions for the enterprise as a whole, and by managing these licenses at the DoD level.

- Consolidate Hardware Purchasing - In parallel with the effort to consolidate software contracting, the Department must also consolidate hardware contracting to the greatest extent practicable in order to address the rising costs of DoD IT and the lack of interoperability that results from uncoordinated IT investments. This will allow the Department to leverage aggregate Department buying power and achieve increased efficiency by securing more favorable contract terms. Further, fewer contracts will require less overhead support, thus generating additional cost avoidance. This initiative will drive procurement of DoD commodity IT hardware (initially desktops, laptops, monitors, servers, printers) through large-scale, proven enterprise-buying processes such as the Air Force Quarterly Enterprise Buy (QEB), the Army Consolidated Buy (CB), and the Marine Corps Hardware Suite (MCHS).

## 5.4 Communications Strategy

The DoD's communications plan for the FDCCI implementation includes close coordination with key internal and external stakeholders. External stakeholders include the Office of Management and Budget, Office of the Director of National Intelligence, the US Coast Guard and public media. Internal stakeholders include all DoD Components. The DoD FDCCI status is regularly briefed to senior DoD leadership at various fora and governance boards. DoD conducts regular coordination (teleconferences / meetings/virtual collaboration sessions) with key stakeholders involved in the FDCCI plan implementation (e.g., end users, support teams, contractors, IT

Infrastructure teams, facilities teams, IT and Agency leadership teams). DoD uses online collaboration tools for disseminating and collecting FDCCI-related information, including the use of Intelipedia/Knowledge Management solutions.

Data center consolidation is a key initiative of the DoD ITESR, which was signed by the Deputy Secretary of Defense on October 5, 2011.

DoD has received many media inquiries on the status of consolidation. Consequently, DoD has is developing public affairs guidance for all DoD Components to ensure that media queries are address rapidly and uniformly. The guidance is being coordinated by the Assistant Secretary of Defense for Public Affairs.

DoD Components have also evolved their own communication strategies. For example, DLA conducts regular, periodic meetings with OSD, DISA and DLA program offices. The Air Force reaches out to DISA on various levels to ensure appropriate development of its long term strategy and goals which include the "DISA First" strategy. Results of these meetings are summarized and passed to leadership and stakeholders across the Air Force. Air Force leadership is continually apprised of progress and FDCCI developments.

# 6 Progress

## 6.1 FDCCI Consolidation Progress

DoD initially identified 52 data centers slated for closure in FY11. Since then, additional 7 data centers were identified for closure in FY11. Of these, all but 4 are on schedule for closure in FY11 for a total of 55 data centers. Hence, DoD has not only met, but exceeded its target for FY11 closures.

DoD is still obtaining updates on FY12 closures. Continuing budget resolutions have delayed the implementation of consolidation plans. Funding is a major risk factor to data center consolidation. Although significant savings are expected in future years, those savings cannot be borrowed to fund required investments for consolidating data centers. Consolidation requires an investment in labor, new and more efficient hardware, upgrades to computer facilities, and increased operating costs when some legacy systems run in parallel with new systems.

DoD has learned several lessons through this initiative. One encouraging sign is the willingness of DoD Components to adopt a 'DISA First' strategy to transfer applications and infrastructure to a shared service provider. Further, a combination of moratoria on hardware acquisition and streamlined acquisition processes are being used to rein in the growth of data centers. DoD is

issuing new policy directing a moratorium on new data centers. As mentioned earlier, DoD will establish Core data centers to support critical enterprise services. The Core data centers will enable further consolidation of legacy data centers in DoD. The Department of the Navy (DON) CIO released the DON Data Center Consolidation Policy Guidance in July 2011 which established a moratorium on all IT investment that would result in creating increased data storage capacity and instead requires the use of existing DON owned enterprise or regional data center capacity first. The Department of the Army CIO/G-6 issued a moratorium on IT spending, dated 8 April 2010 and has issued an execution order for the Army Data Center Consolidation Plan. The Air Force is exploring a policy to centralize the acquisition and funding of commodity IT infrastructure and services, such as application hosting. An Air Force Instruction on Network Operations (NETOPS), is being rewritten to identify those core enterprise services that will be offered as enterprise services. This policy will implement the new centralized acquisition and provisioning strategy that the Air Force is now developing.

DoD has been successful in galvanizing the entire DoD community to develop aggressive targets for data center consolidation. All DoD Components are now engaged in identifying and executing additional opportunities to consolidate. DoD has been able to take advantage of ongoing consolidation efforts such as BRAC-related closures to reduce the data center footprint.

## 6.2 Cost Savings

Calculating cost savings through data center and server consolidation is a challenge. Many IT expenditures are incurred outside the defined IT portfolio and are difficult to track. Presently, many Components in DoD do not capture physical infrastructure and security, building maintenance, or other indirect hosting costs. This is a challenge in determining the cost comparison between Components. Furthermore, IT investments are defined, funded, and operated by individual commands, programs of record, or functional organizations in a decentralized manner. DoD Components are considering new policies to better track costs and identify additional savings. When the Federal TCO becomes available, DoD will use it as a standard tool across the enterprise.

The identification of exact cost savings from these efforts has been difficult. Several factors account for this:

- Personnel/FTE – Many of the personnel involved in management of data centers resources have done so as collateral duties. In other cases, as data centers migrated to other facilities, the personnel were assigned other duties, resulting in no net cost savings.

- Power – Power is not metered at a fine enough level to be able to determine the power expenditures for a given data center, therefore as data centers close, there is no way to measure and identify any power consumption reductions.
- Buildings – in many cases, data center space that became available from FY11 closures was re-purposed for other use, including office space and telecommunication space. No costs savings have been identified from this.
- Hardware/Software – to accept the incoming server, systems and applications, the data center consolidations in FY11 required investment in IT resources at the new site.

Despite these challenges, preliminary estimates suggest that, in the near term, the overall DoD Efficiencies effort, of which data center consolidation is a significant part, will deliver savings of over a billion dollars annually by FY2016 and over three billion dollars over the Future Years Defense Program (FYDP). Specifically, DoD could achieve annual savings of $58 million in energy costs, $511 million in aggregate data center building operational costs, and $111 million in construction and expansion costs by FY15. These figures are approximate and have not been validated by DoD Components and the DoD Comptroller. In particular, these savings do not account for the upfront costs that will be necessary to consolidate. These upfront costs include, but are not limited to, capital investments for new infrastructure, application migration, software and data center infrastructure as well as increased operational costs for more state-of-the-art data centers. Consolidation is expected to result in tangible savings (both direct and indirect costs) in these areas:

- **personnel costs -** fewer support staff needed to maintain servers.
- **infrastructure costs:**
  - **power and cooling**-Less centers and the few that remain operate more efficiently.
  - **workload utilization**-Most data centers historically operate between 15 – 30 %. Consolidation drives this to above 65%.
  - **infrastructure complexity**-Standardized storage, networks and operating systems.
- **real estate**
- **hardware lifecycle costs**
- **technical and functional application support requirements**
- **software licensing circuit/bandwidth requirements, monitoring requirements**
- **information assurance**
- **disaster recovery continuity of operations requirements**