Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap

Version 1.0 – 6 SEP 11

September 2011

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT 05 2011

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 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 of Defense must transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security.

The IT Enterprise Strategy and Roadmap represents the collective efforts of many stakeholders from throughout the Department and presents the DoD Chief Information Officer's (CIO) plan for achieving the goals of increased efficiency, effectiveness, and security. The IT Enterprise Strategy and Roadmap identifies 26 initiatives that will allow the DoD to realize distinct improvements to the DoD Information Environment.

The DoD CIO, in partnership with the DoD Components, is directed to develop initiative implementation plans to provide specific tasks and milestones toward achieving the goals associated with each of the 26 initiatives. These implementation plans are to leverage ongoing efforts and existing DoD Component plans, and to realize for the Department greater capability and efficiency.

This strategy and roadmap requires the active participation of the DoD Components to achieve its intended results. I ask that all Components assist in this effort and support the DoD CIO in increasing the efficiency, effectiveness, and security of the DoD Information Environment and, by extension, providing our Warfighters with the assured access to information and services that they require in order to accomplish their mission of defending our country in the 21st Century.

Foreword

The number of networks the Department of Defense (DoD) uses to execute its missions has increased significantly over the past 30 years. Although these networks have proved vital to DoD's success, the incremental and evolutionary manner in which DoD develops information technology (IT) has resulted in layers of stove-piped systems that are difficult to integrate and not as effective as needed. Although DoD's IT infrastructure enables warfighters to operate effectively in the twenty-first century, the unnecessary complexity of our networks and IT reduces our ability to secure our information systems, hampers our ability to share information, and needlessly consumes the finite resources available to DoD. This untenable situation requires us to make dramatic changes in how we develop, implement, and sustain IT across DoD. Together, we must modify existing processes to reduce complexity and optimize our networks for the joint environment. Our goals are to dramatically increase our cyber security posture, increase our effectiveness across joint and coalition lines, and reduce the resources our networks consume.

This document is our Strategy and Initial Roadmap to achieve these goals and deliver a streamlined, rationalized, and simpler network by consolidating IT infrastructure across DoD. As such, this document also aligns with the U.S. Chief Information Officer (CIO) "25 Point Implementation Plan to Reform Federal Information Technology Management", particularly its call for enhanced operational efficiency. Through this strategy, we are committing to a task that requires changes to policies, cultural norms, and organizational processes to provide lasting results. We will focus initially on obtaining tangible results in Fiscal Years (FY) 2011–2012 and plan for aggressive consolidation through FY2015. Aggressively consolidating now will better position us to embrace emerging technology and provide cutting-edge service to our warfighters. This aggressive consolidation cannot, however, come at the price of degraded capabilities for the warfighter or inflexible commitment to a specific technological solution. Accordingly, this strategy and roadmap is intended to provide DoD with sufficient flexibility to respond to and incorporate emerging technology and to identify and take appropriate actions for those efforts that are not producing.

Our focus remains, as it always has been and always will be, on providing the military forces needed to deter war and to protect the security of our country. This effort will be a collaborative undertaking in which I will work side-by-side with DoD's Component CIO or equivalent IT leads to plan and execute this roadmap and to strengthen the partnerships between the DoD CIO's office and the offices of the Under Secretary of Defense for Acquisition, Technology & Logistics (USD(AT&L)), Director–Cost Assessment and Program Evaluation (D, CAPE), Under Secretary of Defense Comptroller (USD(C)), and Deputy Chief Management Officer (DCMO) to affect long-term change. I look forward to leading DoD through this consolidation effort and delivering a better DoD Information Enterprise in the immediate future.

//signed//

Teri M. Takai

DoD Chief Information Officer

Executive Summary

Historically, DoD's information technology (IT) investments have been made to meet the needs of individual projects, programs, organizations, and facilities. This decentralized approach has resulted in large cumulative costs and a patchwork of capabilities that create cyber vulnerabilities and limit the ability to capitalize on the promise of new developments in IT.

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 DoD's ability to execute its missions while defending its networks against growing cyber threats. Specific direction was received to consolidate IT infrastructure to optimize for the joint environment and to pursue consolidation in a way that does not preclude future consolidation of IT infrastructure at the DoD enterprise level.

During the first quarter of FY 2011, more than 240 representatives from the Office of the Secretary of Defense (OSD), the Military Departments, Defense Information Systems Agency (DISA), National Security Agency (NSA), and United States Cyber Command (USCYBERCOM) analyzed opportunities to consolidate DoD IT infrastructure through specific initiatives in five functional areas: Network Services, Computing Services, Application & Data Services, End-User Services, and IT Business Processes. Detailed descriptions, initial implementation timelines, and rough-order-of-magnitude (ROM) estimates of the required investments and potential savings were developed for 26 initiatives. Each initiative contributes to one or more of the IT Enterprise goals—increase mission effectiveness, improve cyber security, and deliver efficiencies.

Preliminary estimates are that this initial set of initiatives will deliver efficiencies of between $1.2 billion and $2.2 billion annually by FY2016 and between $3.2 billion and $5.2 billion over the Future Years Defense Program (FYDP). This effort already has resulted in a direct budget reduction of $1.7 billion across the FYDP in the FY2012 DoD submission to the President's Budget through specific IT consolidation actions by the Air Force ($1.2 billion) and the Army ($500 million).

The DoD Chief Information Officer (CIO) Executive Board (CIO EB) is DoD's senior functional oversight body for IT infrastructure and will be the focal point for IT consolidation governance.

The Components' progress against their IT consolidation performance measures will be reported through the CIO EB to the Deputy's Advisory Working Group (DAWG) and the Defense Business Systems Management Committee (DBSMC) as appropriate.

Specific changes to DoD's three core processes—Joint Capabilities Integration and Development System (JCIDS), Planning, Programming, Budgeting and Execution (PPBE), and Defense Acquisition System (DAS)—are required to address the systemic conditions that lead to DoD's stove-piped IT infrastructure. The DoD CIO will work with the core process owners to implement the required changes. These efforts will be synchronized with the parallel DoD activities under way to reform DoD IT acquisition.

Effective communication is critical to building the DoD-wide commitment that will be required to optimize DoD IT infrastructure for the joint environment. This document is the initial communication of the Secretary's intent and will be followed by communications that detail associated policy, performance measures, architectures, and standards.

Table of Contents

List of Figures

This page intentionally left blank.

1 Introduction

In August 2010, the Secretary of Defense (SecDef) announced a Department of Defense (DoD)–wide Efficiencies Initiative to move America's defense institutions toward a "more efficient, effective, and cost-conscious way of doing business."[1] DoD Components were directed to conduct a "zero-based review" of how they carry out their missions and of their priorities, and to rebalance resources to better align with DoD's most critical challenges and priorities. As part of the announcement, the SecDef directed consolidation of information technology (IT) infrastructure assets to achieve savings in acquisition, sustainment, and manpower costs and to improve DoD's ability to execute its missions while defending its networks against growing cyber threats.

In response, DoD established an IT Consolidation Task Force to analyze alternative courses of action (COA) and recommend specific IT infrastructure consolidation initiatives. Three COAs were developed:

COA 1–Consolidate IT infrastructure at the DoD Component level
COA 2–Consolidate IT infrastructure to optimize the joint environment
COA 3–Consolidate IT infrastructure at the DoD enterprise level

A November 2010 in-process review resulted in SecDef direction to consolidate IT assets to optimize the joint environment (COA 2) and to pursue the consolidation in a way that does not preclude future consolidation at the DoD enterprise level (COA 3). To "optimize for the joint environment" is to create a seamless DoD Enterprise Information Environment (EIE), which will support cross-organizational, geographically dispersed users through the delivery of IT infrastructure capabilities. In this context, DoD users worldwide at all services, agencies, commands, and activities are part of the joint environment.

The EIE is composed of Global Information Grid (GIG) assets that operate as, provide transport for, or assure networks at all levels. The EIE Mission Area (EIEMA) is the DoD IT portfolio that manages investments in the information sharing, computing, and communications environment of the GIG. The EIE includes computing infrastructures and common enterprise services that provide users with the ability to access and use information on the GIG. The consolidation of the IT infrastructure described in this plan will replace Service- and installation-specific IT infrastructure capabilities and processes with the intention of optimizing DoD's IT infrastructure, increasing mission effectiveness, improving cyber security, and reducing cost in accordance with SecDef direction. DoD will seek to garner efficiencies and to increase effectiveness of the DoD IT infrastructure across all Military Departments, Combatant Commands (COCOM), and Agencies.

[1] Gates, Robert M., (2010). *Statement on Department Efficiencies* Initiative. Accessed from: http://www.defense.gov/speeches/speech.aspx?speechid=1496

2 Background

DoD is an immense and complex organization. It has more than 1.4 million men and women serving on active duty, employs 750,000 civilian personnel, and counts another approximately 1.1 million in the National Guard and Reserve, making it the nation's largest employer (Figure 2-1). In addition, more than 5.5 million family members and military retirees receive benefits as a result of their past service or their relationship to a service member. Supporting the diverse IT needs of this population is a tremendous challenge that involves more than 15,000 classified and unclassified networks, more than 7 million computers and IT devices, and a 170,000-person IT workforce.

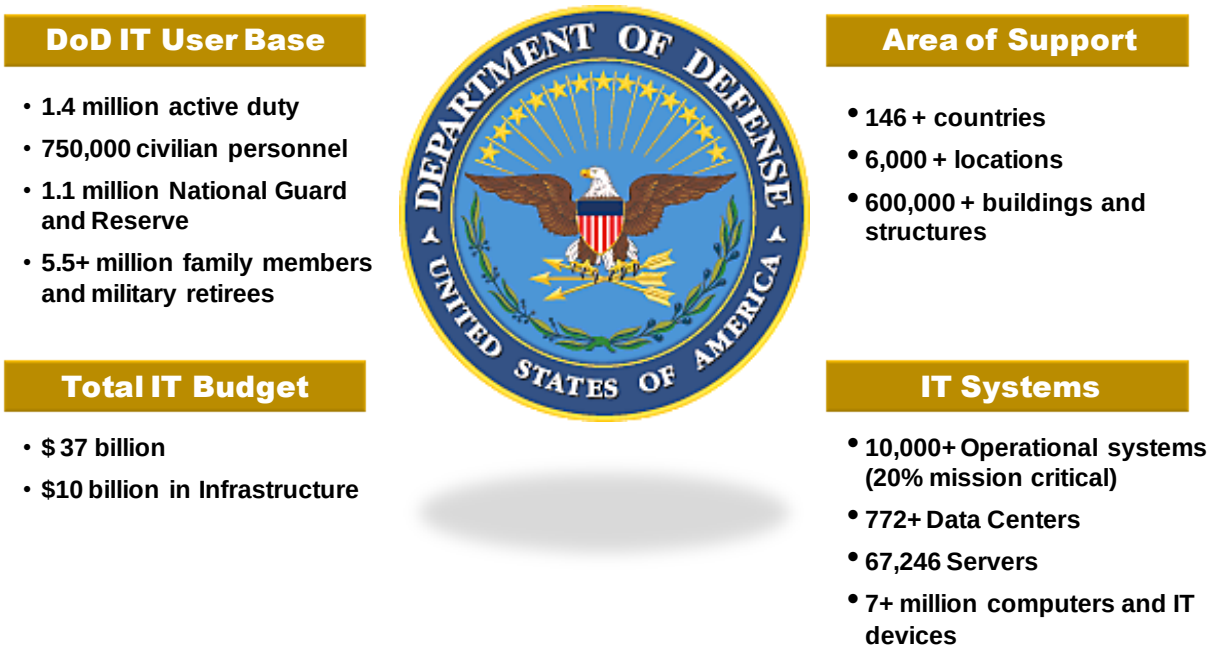

Figure 2-1: DoD IT Infrastructure Characteristics

DoD depends on timely, accurate, and focused information at every echelon across the full range of military operations (ROMO), Joint Operations Concepts (JOpsC), Joint Integrating Concepts (JIC), and Joint Functional Concepts (JFC).[2] Achieving and maintaining the information advantage as a critical element of national power requires the concentrated effort of the entire DoD to provide an information environment optimized for the warfighter and effective for all echelons, from the tactical edge to the strategic core. Unfortunately, the way DoD networks are developed, funded, and implemented fosters unnecessary complexity and redundancy. As a result of this decentralized approach and lack of governance and oversight, DoD's IT infrastructure delivers a patchwork of capabilities that creates cyber vulnerabilities, impedes joint operations, results in large cumulative costs, and limits the ability to capitalize on the promise of IT.

In addition to enhancing DoD networks to better support DoD's information needs, this strategy and roadmap also focuses on providing better support for mission partners and interoperability in a joint environment. The global reach of the United States and its position of prominence in

[2] Joint Staff J7. (2010). *J7 Joint Force Development and Integration Division (JFDID)*. Accessed from: http://www.dtic.mil/futurejointwarfare/index.html

global affairs dictate that DoD does not operate in a vacuum. As a result, success is ensured by operating in conjunction with domestic agencies and federal departments, armed forces and governments of foreign countries, and international non-governmental agencies. Regardless of the spectrum in which DoD is operating, from disaster relief to full kinetic warfare, the information environment must support collaboration and information sharing to be effective.

3 Vision for a more Effective, Efficient and Secure DoD Information Enterprise

Twenty-first century military operations require an agile information environment to achieve an information advantage for personnel and mission partners. To achieve this information advantage, everyone in DoD must be able to access the information resources they require to perform their required functions on any computer on DoD networks anywhere in the world, consistent with security classification and special access restrictions. To meet this challenge, DoD is undertaking a concerted effort to unify its networks into a single information environment that will improve both operational effectiveness and information security posture, while also achieving efficiencies that allow resources to be redirected to meet mission needs.

3.1 Improving Effectiveness

In the envisioned end state, users will have timely access to the information and resources they require, anywhere and anytime across the DoD Information Enterprise (IE), enabling them to make informed decisions in executing their missions. Therefore, the GIG will be designed and optimized to more effectively and efficiently support mission operations, for both garrisoned users and those at the edge. For example—

- Decision makers across DoD will have seamless access to functionality, enabling them to create, find, use, and share information needed to perform their assigned tasks. This access will be made available for use on a wide variety of fit-for-purpose mobile devices.
- Commanders will have access to information available from all DoD resources, enabling improved command and control (C2), increasing speed of action, and enhancing the ability to coordinate across organizational boundaries or with mission partners.
- Individual service members and government civilians will be provided with a standard IT user experience, enabling them to do their jobs and providing them with the same look, feel, and access to information on reassignment, mobilization, or deployment.
- Common identity management, access control (including single sign-on [SSO]), authorization, and authentication schemes will enable broader access to information and services. Access to information will be based on a user's credentials and needs rather than on the user's physical location. Common networks will remove access and performance barriers imposed by organizationally stove-piped networks.
- Common DoD-wide services, applications, and tools will be broadly usable across the DoD, thereby minimizing duplicate efforts, reducing data fragmentation and translation, and reducing the need for retraining when users are reassigned, mobilized, or deployed.
- Streamlined IT acquisition processes will support rapid fielding of capabilities. In addition, enterprise-wide certification and accreditation (C&A) will speed the implementation and availability of new services and applications.
- Consolidated operations centers will enable dynamic allocation of garrisoned and deployed network resources to provide computing resources and bandwidth as needed. Fewer, more standardized data centers will make it easier to access, reallocate, and monitor resources. Greater asset visibility will enable better utilization and security.

A consolidated network environment, with global visibility to information assets, will enable dynamic allocation of resources in response to cyber threats and more effectively maintain network performance.

3.2 Improving the Information Security Posture

As DoD consolidates its disparate networks, it will dramatically improve the security posture of its information assets, as follows:

- Consolidation will better enable secure mission-driven access to information and services, rendering DoD information securely accessible to all who need it and are authorized access to it. Deploying an enterprise identity, authentication, authorization, and access management service will extend security protection from the network to the data on the network, providing security controls to better enable secure information sharing.
- DoD networks will be better protected from threats, both internal and external, that will continue to attempt to exploit seams in DoD's information infrastructure to gain and maintain access and act against national interests. IT Infrastructure Consolidation will reduce the number of networks and data centers, thereby reducing the number of vulnerable seams. In addition, enhanced computer network defense (CND) capabilities will enable DoD to better anticipate and prevent successful attacks on data and networks.
- In this highly contested environment, implementing processes, technology, information management, and agile command structures will ensure that U.S. military networks and information resources remain available on a trusted and secure network. Ensuring readiness levels are sustained and enterprise capabilities are recovered quickly from any event will enable preparation for, and operation through, attacks on or degradation of the DoD information environment.

3.3 Enabling Efficiencies

The consolidation of DoD's networks, combined with increased use of enterprise-wide solutions, will bears the potential to reduce IT costs across DoD. Although many elements of IT infrastructure, applications, and services will continue to be owned and operated by individual Components, they will be developed, maintained, and operated in compliance with strictly enforced standards. This will ensure maximum operational effectiveness and security while minimizing unnecessary duplication and redundancies. Every new capability brought onboard will be easier to acquire because it will operate within a set of consistent and well-understood enterprise standards and will interface with fewer functionally overlapping services and applications. Thus, the end state not only will result in effective and secure information resources, but also will deliver a DoD Information Enterprise that is significantly less expensive to build, maintain, and operate. This IT Enterprise Strategy and Roadmap represents a first step toward achieving this vision.

4 IT Enterprise Strategy

An effective military strategy can be expressed as "*Strategy = Ends + Ways + Means*" where "Ends" refers to the end-state objectives or goals; "Ways" are the actions required to reach the end state; and "Means" are the resources needed to execute the actions.[3] The "Ends" of DoD's IT Enterprise Strategy are detailed in Section 4.1. Sections 4.2–4.5 describe the "Ways" and "Means" that are necessary to achieve the "Ends." Section 7 details the sustaining processes needed to ensure that the "Means" are available as well as the changes to those processes that are required to facilitate IT consolidation efforts.

4.1 IT Enterprise Goals

The DoD IT Enterprise Goals are focused on increasing mission effectiveness, improving cyber security, and delivering efficiencies. Figure 4-1 depicts the key benefits and relationships of these goals and illustrates the realm in which the IT Enterprise Strategy seeks to coordinate execution of DoD IT to obtain the best results for the warfighter and DoD as a whole.

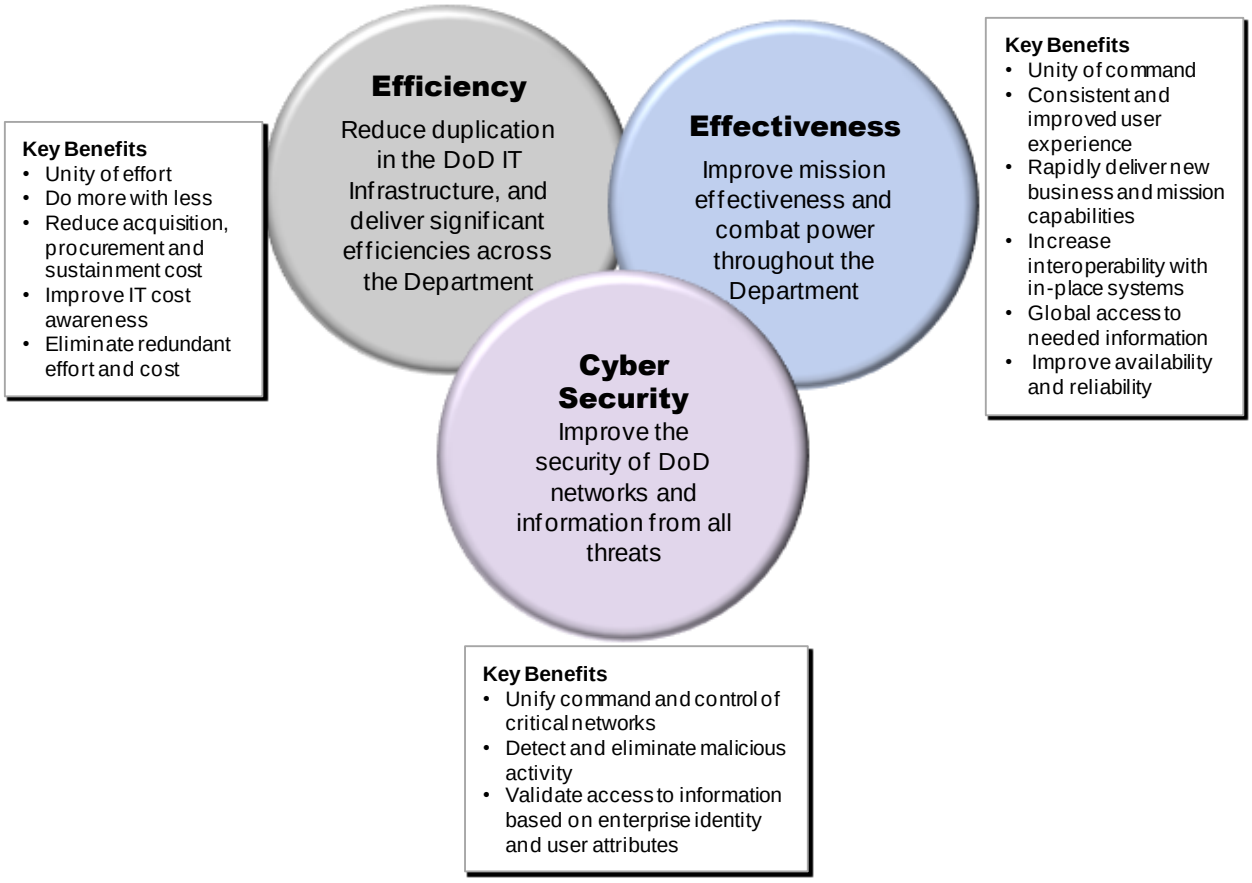

Figure 4-1: IT Infrastructure Enterprise Goals

The result of these consolidation initiatives will be a DoD Information Environment that can provide the warfighter with the required information and services in a seamless manner. Such a standardized information and network infrastructure will eliminate the organizational barriers to

[3] Arthur F. Lykke Jr., ed., (1998). Military Strategy: Theory and Application. Carlisle, Pa.: U.S. Army War College.

information sharing and, as a result of this standardization, eliminate seams that attackers can exploit to gain access to vital information or systems. The consolidation and standardization activities outlined in this document also will improve the flexibility of defense networks by minimizing the organizational and technological changes needed to incorporate or respond to changes in emerging technology.

4.1.1 Improve Mission Effectiveness

The National Defense Strategy of June 2008 highlights the importance of information sharing to national security.[4] The strategy notes that providing secure, assured, and reliable information requires not only technological changes, but also changes that break down the cultural barriers impeding progress. Nowhere is this cultural challenge more evident than in the current approach to IT infrastructure provisioning.

In today's environment, the Combatant Commands (COCOM) are provided with Service-centric IT networks and IT services focused on Service–unique domains. This Service-centric approach extends beyond networks to identity and access management processes, data centers, mission and business applications, commercial off-the-shelf (COTS) hardware and software, and IT procurement practices. The result is an IT infrastructure that does not effectively support the joint warfighting environment.

The need to improve DoD's IT infrastructure to support the joint warfighter is well documented. In June 2009, the Joint Requirements Oversight Council (JROC) approved the Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD).[5] The accompanying GIG 2.0 Concept of Operations (CONOPS) outlines a future of "a single information environment with common standards and centralized governance providing the information advantage to warfighting commanders."[6] The GIG 2.0 concept transforms the current understanding of the GIG from a coalition of departments and agencies with their own sets of systems, processes, governance, and controls to a more seamless, unified, and integrated net-centric environment.

An initial assessment by the Joint Staff indicates that the IT consolidation initiatives described in this document address 24 of the 66 GIG 2.0 ICD capability gaps, with emphasis on joint infrastructure and enterprise services. Many of the remaining GIG 2.0 capability gaps are currently being addressed by non-material (i.e., policy and doctrine) activities.

These documents and studies serve as the foundation on which DoD can develop the capabilities to—

- Provide assured access to required quality information from a seamless, survivable, and durable information environment with a focus that spans from the warfighter at the tactical edge back to the core IT infrastructure
- Provide a unified network environment that simplifies the synchronization and integration of intelligence collection, processing, exploitation, analysis, and dissemination to meet the information requirements of military decision makers
- Optimize network capabilities for the joint force that scale from the tactical to the strategic levels

[4] Department of Defense. (2008). National Defense Strategy. Accessed from http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf
[5] Joint Staff J6. (2009). Global Information Grid 2.0 Initial Capabilities Document, JROCM 095-09.
[6] Joint Staff J6. (2009). The Global Information Grid 2.0 Concept of Operations Version 1.1.

- Improve communications and understanding through information sharing with mission partners
- Improve situational awareness and force protection by providing reliable and timely access to required information

DoD's IT infrastructure must be simplified to an integrated and interoperable resource that quickly delivers the right information at the right time to the right place anywhere in the world.

4.1.2 Improve Cyber Security

Another key focus of the DoD IT Enterprise initiative is to enhance DoD's ability to counter cyber security threats. DoD networks are under constant attack from cyber security threats launched from the Internet or from malicious software embedded in e-mail attachments, removable media, or embedded in the hardware DoD procures. Every connected device is susceptible to cyber vulnerabilities. In addition to these threats, DoD networks also must be prepared for malicious actors operating from inside the organization.

At the root of DoD's cyber security challenge is the size and complexity (i.e., configuration variance) of legacy network infrastructures and software systems. As information needs expanded, new systems—many with their own dedicated networks—were added to support DoD missions. Virtual networks were layered on top of physical networks and independent access control approaches were developed as organizations worked to protect their systems and networks. This has led to a DoD information environment where systems, networks, and standards are deployed in a patchwork manner and the security of the entire enterprise is susceptible to exploitation through the areas with the weakest protection.

Specific IT consolidation initiatives will be undertaken to—

- Improve cyber security situational awareness and command and control
- Establish processes for granting access to networks and systems access using validated cryptographic identity credentials
- Detect "anomalous behavior" inside DoD networks (e.g., malicious software, unauthorized data movement)
- Manage configurations and automate compliance monitoring and enforcement
- Reduce or eliminate the need to manually download information onto removable media to move it to another security domain
- Streamline certification and accreditation
- Establish processes and develop capabilities to protect and defend DoD networks as a single information environment

4.1.3 Deliver Efficiencies

DoD spends more on IT annually than any other department or agency, accounting for almost half of the $78 billion government-wide IT budget in FY10. The FY10 IT DoD budget was more than $37 billion and included more than 5,800 separate funding lines.[7] More than $10 billion

[7]Department of Defense. (2009). National Defense Budget Estimates for FY2010. Accessed from: http://comptroller.defense.gov/defbudget/fy2010/Green_Book_Final.pdf

annually is spent developing and sustaining IT infrastructure capabilities (e.g., data centers, networks, software applications, desktops, and mobile devices).

DoD has an obligation to ensure that IT services are delivered in the most cost-effective and efficient manner possible. The private sector and state and local governments have demonstrated that leveraging shared services and consolidating IT and telecommunications equipment, resources, and investments can improve efficiency, cost-effectiveness, and environmental sustainability in IT and telecommunications operations. DoD's IT consolidation activities will optimize DoD investments in IT infrastructure while also increasing mission effectiveness and improving cyber security. Specific initiatives will—

- Reduce procurement and sustainment costs
- Leverage economies of scale to increase buying power
- Reduce energy use

4.2 Governance

An effective DoD CIO governance structure begins with strong CIO-driven leadership to establish direction and hold the DoD IT organizations accountable. In today's complex DoD IT environment, leadership must provide effective governance to manage technology in support of business needs and mission effectiveness. This governance includes the structures and processes for setting direction, establishing standards, and prioritizing IT investments. Proper governance will enable DoD to leverage a framework for accountability in enforcing compliance with decisions about technology use and procurement.

The DoD CIO has primary responsibility for developing and enforcing DoD's overall IT policy, architecture, and standards; Component CIOs are accountable for implementing and complying with DoD CIO direction. Both the DoD CIO and the Component CIOs are responsible for overseeing IT investment management and information assurance (IA) in compliance with the Clinger-Cohen Act (CCA) and the Federal Information Security Management Act (FISMA). The DoD CIO will leverage the DoD CIO Executive Board (EB), and its reporting relationship to the Deputy's Advisory Working Group (DAWG), and the Defense Business Systems Management Committee (DBSMC) as the focal points for DoD IT consolidation.

The CIO EB will serve as DoD's senior functional oversight forum, where IT consolidation matters are vetted for input to planning, programming, budgeting, and execution (PPBE), the Defense Acquisition System (DAS), and the DAWG for approval. Components will submit their aligned IT consolidation implementation plans to the DoD CIO EB and their progress will be tracked, consolidated, and briefed to the DAWG through this forum. Components also are to report the impact of the IT consolidation initiatives on end users when reporting on the progress of the initiatives. Based on these reports, the DAWG will be able to direct the initiation, suspension, or termination of initiatives based on performance, the emergence of new technology, or other changes internal or external to DoD. The necessary subordinate groups needed to produce policy, standards, architecture, and guidance will be formed under the direction of the CIO EB.

Figure 4-2 shows the tiered structure that IT Enterprise governance will follow.

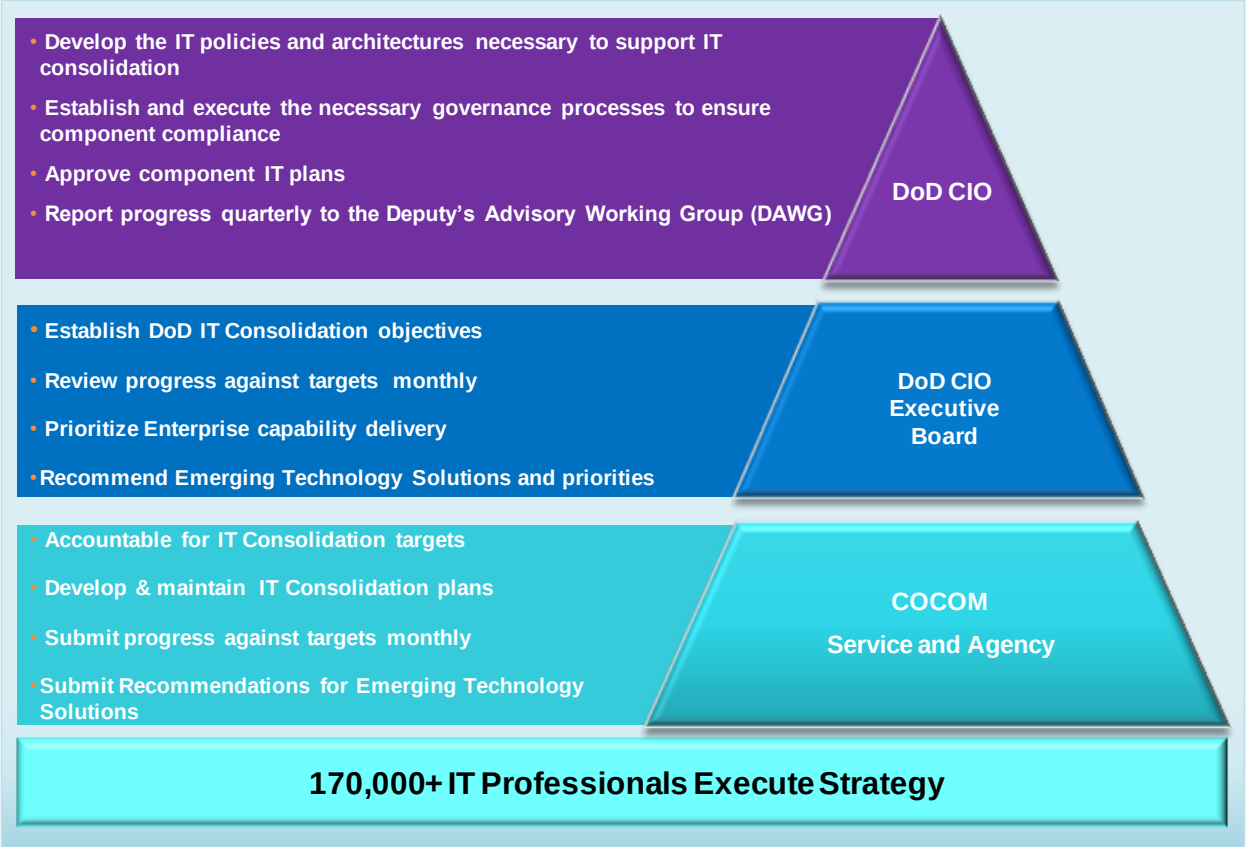

Figure 4-2: DoD IT Enterprise Governance Framework

4.3 Management Approach

DoD will use a "tiered accountability/modest federation" approach to IT consolidation. Under this approach, responsibility and accountability for implementing IT consolidation initiatives are assigned to different levels within the organization. For example, the DoD CIO is responsible for developing the *enterprise* IT policies and architecture (i.e., DoD-wide policies, capabilities, standards, reference architectures, and rules) and the associated *enterprise* IT Enterprise Strategy and Roadmap. Each Component is responsible for producing a *Component*-level architecture and IT consolidation plan associated with its own tiers of responsibility in a manner that is aligned with (i.e., does not violate) the enterprise IT policies and architecture. Similarly, program managers are responsible for developing *program*-level architectures and consolidation plans and for ensuring alignment with the enterprise-level and Component-level architectures and plans above them. This structure provides flexibility while also ensuring linkages and alignment from the program level through the Component level to the enterprise level.

Centralized management, however, will be used to achieve a number of efficiencies. For example, the DoD CIO will provide specific guidance in terms of product lists, product configurations, and, in some cases, the specific products or services themselves. The DoD CIO also will establish appropriate governance and resourcing processes to ensure that the centrally managed capabilities meet the mission needs of the individual Components.

4.4 Initial Performance Metrics

The Components' progress against IT Enterprise objectives will be measured against the key drivers that impact mission effectiveness, cyber security, and efficiency. Initial measures will focus on—

- The number of data centers and servers
- The percentage of server capacity being used
- The number of physical and logical networks
- The percent of mission-critical applications using the enterprise attribute-based access control capability
- The dollar value flowing through designated DoD-wide COTS hardware and software procurement mechanisms

The measures listed above are illustrative only and are presented to highlight DoD's focus on key drivers and on only those items that DoD Components can count. The actual measures selected for use will depend on which initiatives are approved through DoD's processes. Final IT Enterprise metrics will be vetted by the CIO EB and presented to the DAWG for approval. Focusing metrics on the key drivers will illuminate lower-level implementation issues without placing undue reporting burdens on the Components.

4.5 Communications Plan

An effective communications plan is critical to building DoD-wide commitment to the IT Enterprise Initiative. Given that commitment, the communications strategy is targeted at moving staff along the commitment curve depicted in Figure 4-3.[8]

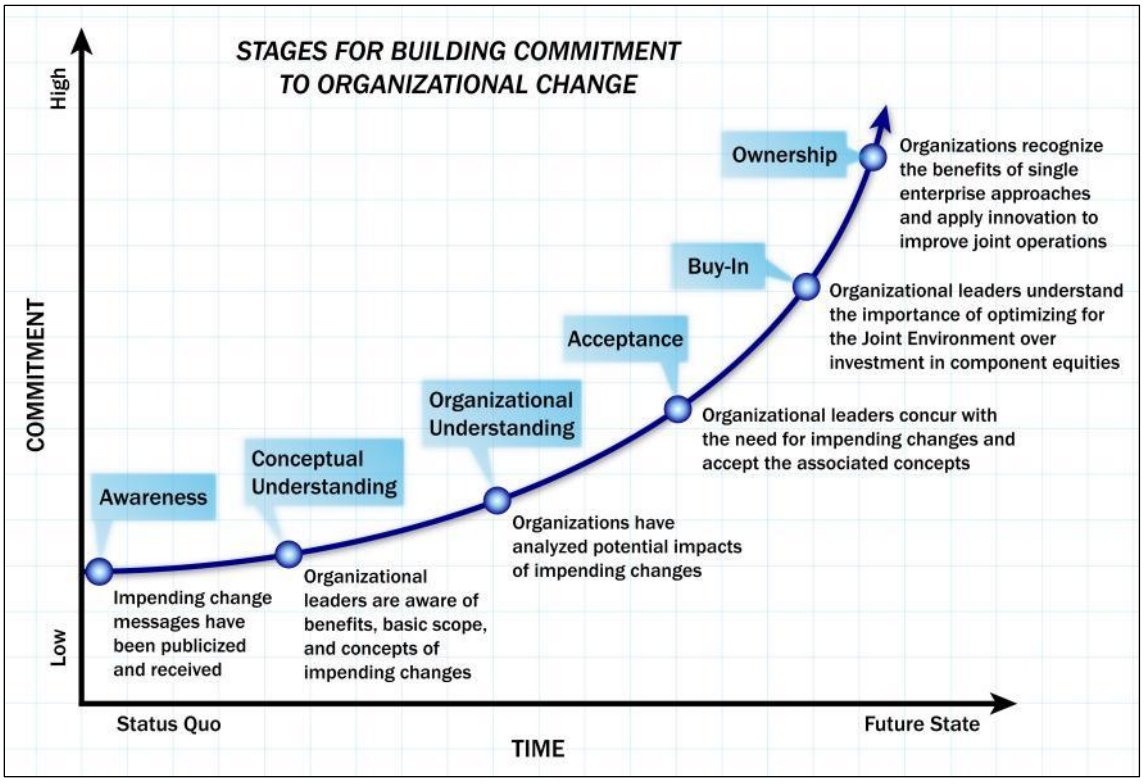

Figure 4-3: Building Commitment

[8] Adapted from the Commonwealth of Massachusetts IT Consolidation Communications Plan. See http://go.usa.gov/Yat

In addition to the framework provided by the commitment curve, the communications strategy will be constructed using the following guiding principles:

1. Recruit leaders (e.g., COCOM Commanders, Military Department CIOs, Agency CIOs) and use existing working groups (e.g., DAWG, DBSMC, CIO EB) to serve as communications champions
2. Distribute communications in a tiered fashion—a message is created centrally and passed down in a consistent manner through each level of leadership—to build message consistency and allow for delivery from the appropriate leader for each stakeholder group
3. Provide timely updates that are appropriately scoped for each stakeholder group throughout the entire consolidation process
4. Incorporate a two-way communications process, providing stakeholders with mechanisms to ask questions, offer feedback, and raise issues
5. Establish a procedure for addressing issues and communicating the results to stakeholders in a timely fashion
6. Develop messages that detail how initiatives address stakeholder needs and concerns
7. Conduct the planning, budgeting, and governance in a transparent way that ensures a balanced and non-duplicative set of IT capabilities are provided by a set of Component implementation plans

The expected benefits of the strategy include consistent messaging throughout the process, well-informed stakeholders, and coordinated efforts across DoD.

5 IT Enterprise Roadmap

In accordance with the SecDef's direction to consolidate DoD IT infrastructure, the DoD CIO established working groups to identify specific initiatives that align with the IT Enterprise goals of increasing mission effectiveness, improving cyber security, and delivering efficiencies. More than 240 representatives from Office of the Secretary of Defense (OSD), the Military Departments, DISA, NSA, and USCYBERCOM identified a set of initiatives that map to the IT Enterprise goals, as shown in Figure 5-1. The initiatives are grouped in the following functional areas:

- **Network Services (NS):** Services (including hardware, software, and labor) that provide telecommunications (i.e., voice, video, and data transport), including inter-installation (long-haul) networks, installation campus area networks (ICAN), and network management and IA services
- **Computing Services (CS):** Services that provide the ability to process, store, and access information, including data centers and servers, storage, and other hardware inside of them
- **Application and Data Services (ADS):** Common shared applications, services, and processes
- **End-User Services (EUS):** Specific subset of computing services that enable end users to access information applications and services locally and via the network
- **IT Business Processes (BP):** Processes used to procure the hardware, software, and services needed to operate and maintain the DoD IT infrastructure

Detailed descriptions, initial implementation timelines, and rough-order-of-magnitude (ROM) estimates of required investments and potential savings were developed for each initiative. Technical and cultural risks were assessed on a scale of high, medium, and low.

The following sections describe the technical approach to consolidation for each functional area. Brief descriptions of each initiative are provided in Appendices A–E. Technical dependencies among initiatives have been identified and will be factored into detailed implementation plans.

	Increase Mission Effectiveness	Improve Cyber Security	Deliver Efficiencies	Technical Risk	Cultural Barriers
Network Services (NS)					
NS1: Consolidate Security Infrastructure	★	★	★	Medium	High
NS2: Consolidate NetOps Centers	★	★	★	Medium	High
NS3: Cross Domain Enterprise Service	★	★	★	Medium	Low
NS4: Standard C&A Process	★	★	★	Low	High
NS5: Extend Joint Networks Over SATCOM	★	⋆	★	Low	Low
NS6: Video Over IP	⋆		★	Low	Medium
NS7: Voice Over IP	⋆		★	Low	Medium
NS8: Joint Enterprise Network	★	★	★	Low	Medium
NS9: Network Infrastructure Reliability	★			Medium	Low
NS10: Defense Red Switch Network (DRSN)	⋆		★	Low	Low
Computing Services (CS)					
CS1: Consolidate Data Centers and Servers	⋆	★	★	Medium	Medium
CS2: IT Infrastructure and Services Optimization	★	★	★	Medium	High
CS3: Cloud Computing	⋆	⋆	★	Medium	High
CS4: Service Desk Consolidation and Optimization	⋆		★	Medium	High
End User Services (EUS)					
EUS1: Next-Gen End User Devices		★	★	Medium	Medium
EUS2: Multi-Level Security Domain Thin Client	★	★	★	Medium	Low
EUS3: Interoperability within DoD and between Mission Partners	★	★	★	Medium	Medium
Application and Data Services (ADS)					
ADS1: Enterprise Messaging and Collaboration (including Email)	★	★	★	Medium	Medium
ADS2: Identity and Access Management Services	★	★		Medium	Medium
ADS3: Enterprise Services Platform	★	⋆	★	Low	High
ADS4: Enterprise Records Mgmt	⋆		★	Low	Low
IT Business Processes (BP)					
BP1: Consolidate COTS Software Purchasing			★	Low	Medium
BP2: Consolidate COTS Hardware Purchasing	⋆	★	★	Low	Medium
BP3: Optimize IT Service Purchasing	★		★	Low	High
BP4: Common Business Process Foundation	★		★	Medium	High
BP5: Promote and Adopt "Green" IT			★	Low	Medium

★ Significant Contribution
⋆ Some Contribution

Figure 5-1: IT Consolidation Initiatives

5.1 Initial Consolidation Initiatives

In order to take advantage of existing efforts and to focus the limited resources of the DoD on achieving tangible gains in the near-term, the DoD CIO coordinated with the Services to identify a subset of initiatives which will be addressed in an initial implementation plan. These initiatives, along with their overarching timelines, are shown in Figure 5-2. This initial implementation plan will provide guidance on the means by which the Department will realize the goals of the selected initiatives while also preparing planning activities for those initiatives which will require long-term efforts.

To the greatest extent possible, the initiative implementation plans will utilize existing working groups, pilot programs, and other efforts already underway to address the issues presented in the initiatives. Additionally, business case analyses will be developed for each initiative to support CIO EB assessment and DoD decision-making processes.

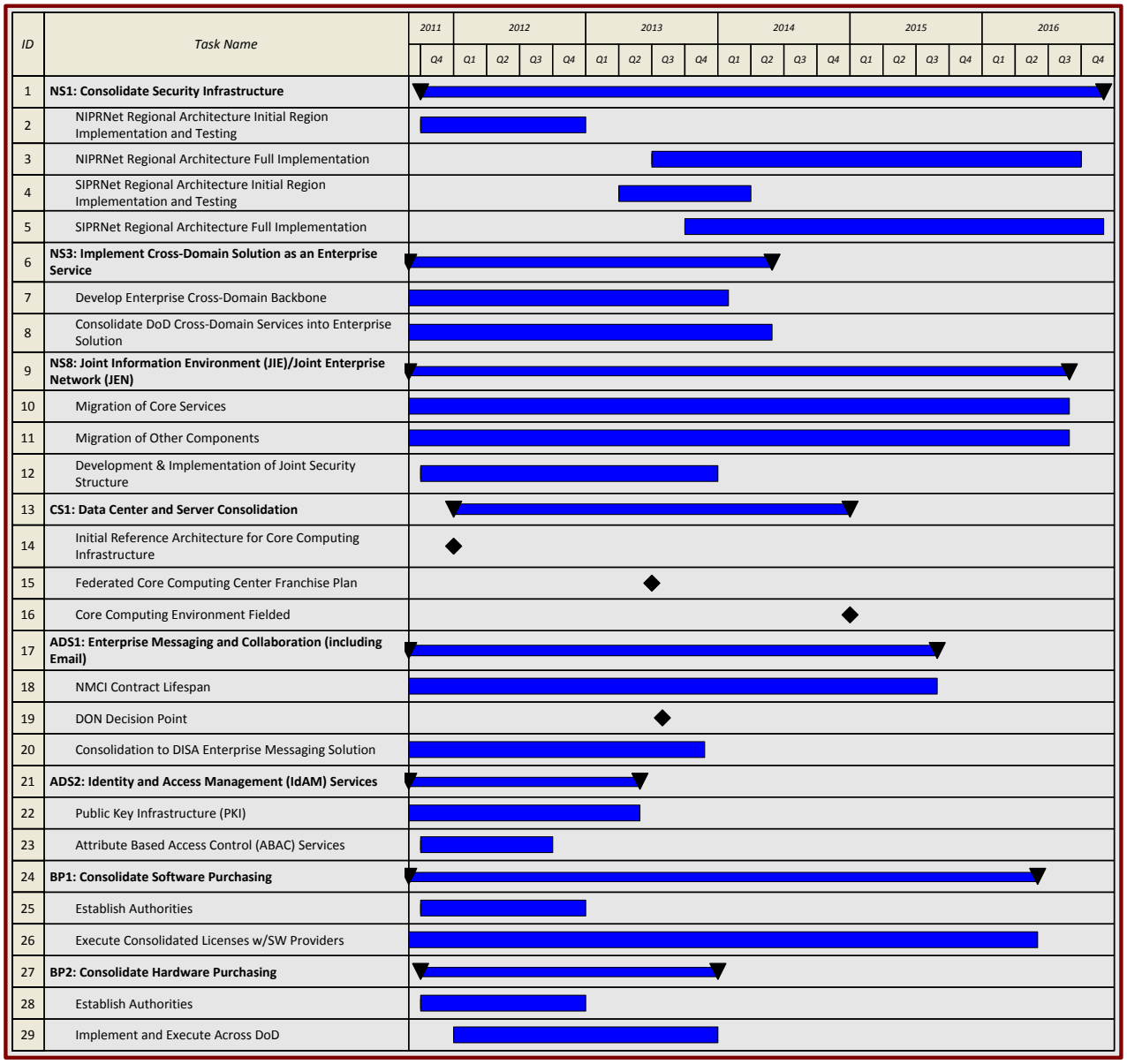

Figure 5-2: Initial IT Consolidation Initiatives

5.1.1 Network Services (NS)

Today, thousands of individual programs, including formal programs of record and informal "projects," maintain private network enclaves. Each of these individual networks has separate support staff, including network operators, administrators, and IA personnel. In addition, each individual network maintains a "security stack" that often is unique to that program. The direct and indirect cost of all the hardware, software, and labor required to operate and maintain these individual program, organization, and installation networks is substantial. The individual networks significantly detract from or completely negate the ability to securely share information across the enterprise and/or to execute effective C2 of DoD networks. As a result, the effectiveness, agility, and security of geographic COCOM and Combined Joint Task Force commanders' networks are significantly degraded.

The three military departments (MilDeps) already have begun taking actions to consolidate their networks, but these efforts must be accelerated and synchronized to ensure maximum effectiveness, cyber security, and efficiency are achieved at the enterprise level.

DoD's approach to eliminating unnecessary costs and improving network capabilities as noted above is to—

1. Consolidate operations and maintenance (O&M) of network services on each DoD installation to the greatest extent practical
2. Accelerate consolidation of internal networks by eliminating the individual networks currently maintained by programs, organizations, and local facility managers
3. Replace program-, organization-, and installation-level security services and infrastructure with a suite of enterprise-level security services, including separate Public Key Infrastructure (PKI)–enabled, attribute-based access control services for devices and for people
4. Strictly enforce compliance with all DoD enterprise-level guidance for IA and cyber security

5.1.2 Computing Services (CS)

Recent advances in computing technologies have sparked a revolution in the provision of computing resources through the ready access of computing as an on-demand service. This enables shared and distributed computing approaches that can accelerate DoD's efforts to achieve net-centric operations by ensuring that warfighters receive the right information and applications from trusted and accurate sources, when and where they need it. DoD recognizes that leveraging these advances will enhance C2 and combat support capabilities for warfighters and decision makers, thereby increasing operational effectiveness. DoD's future computing environment will securely leverage and share the full range of available physical and virtual computing resources in a rapid and demand-based manner across the complete spectrum of strategic, operational, and tactical missions.

Unfortunately, the current state of IT procurements, coupled with the relatively low cost of IT hardware, makes it possible for many entities within DoD to purchase and operate their own computing infrastructure. As a result, the DoD information environment is overly complex and susceptible to exploitation through these myriad devices, systems, and standards by malicious actors intent on causing harm to national interests. Accordingly, DoD will pursue consolidation of computing services with four major efforts during the next 24 months:

1. Merge and eliminate non-MilDep IT infrastructures as appropriate, thereby creating economies of scale that can be leveraged to obtain the best value for DoD.
2. Centrally manage and restrict the diversity of "server (development and operational) platforms" used throughout DoD and require all commodity hardware (e.g., servers, server operating systems, and storage area networks) to be purchased through a limited number of consolidated contracts that leverage economies of scale to reduce total cost to the enterprise.
3. Establish a Core Computing infrastructure that will provide assured and ubiquitous access to vital enterprise services.
4. Aggregate computing services and consolidate infrastructure requirements to gain economic efficiencies of scale whenever practical, such as consolidating regional land mobile radio (LMR) infrastructure or contracts for office printer maintenance and ink cartridges.

Consolidation of IT infrastructures will result in a hierarchy of DoD data centers based on functionality, purpose, and efficiency. Initial DoD plans will result in—

- 32% reduction in data centers
- 30% reduction in racks
- 25% reduction in servers

DoD plans to further reduce the number of data centers to 428 by FY15 (32% reduction from FY10), as directed in the FY12 OMB Budget Passback.

The objective is to consolidate computing services into one of three computing center facilities: 1) Enterprise Computing Centers (ECC); 2) Area/Regional Processing Centers (A/RPC); or, 3) Installation Processing Centers (IPC) as shown in Figure 5-3.

Enterprise Computing Center (ECC): ECCs are designated by the DoD CIO and may be operated by either the Defense Information Systems Agency (DISA) or a Service. ECCs will comply with enterprise-level standards and host applications from any DoD Component based on agreed-on service-level agreements. ECCs are the preferred and default location for all DoD servers.

Area/Regional Processing Center (A/RPC): A/RPCs are designated by the DoD CIO and may be operated by either the Defense Information Systems Agency (DISA) or a Service. The DoD CIO, in collaboration with COCOMs, designates A/RPCs to host systems that must have either a primary or back-up instantiation in a particular location for technical, operational, or financial reasons.

Installation Processing Center (IPC): With approval of the DoD CIO, an installation may utilize an IPC to host systems that require local instantiation for operational or technical reasons.

Components will develop plans to relocate existing computing center facilities into one of the three types of facilities described above.

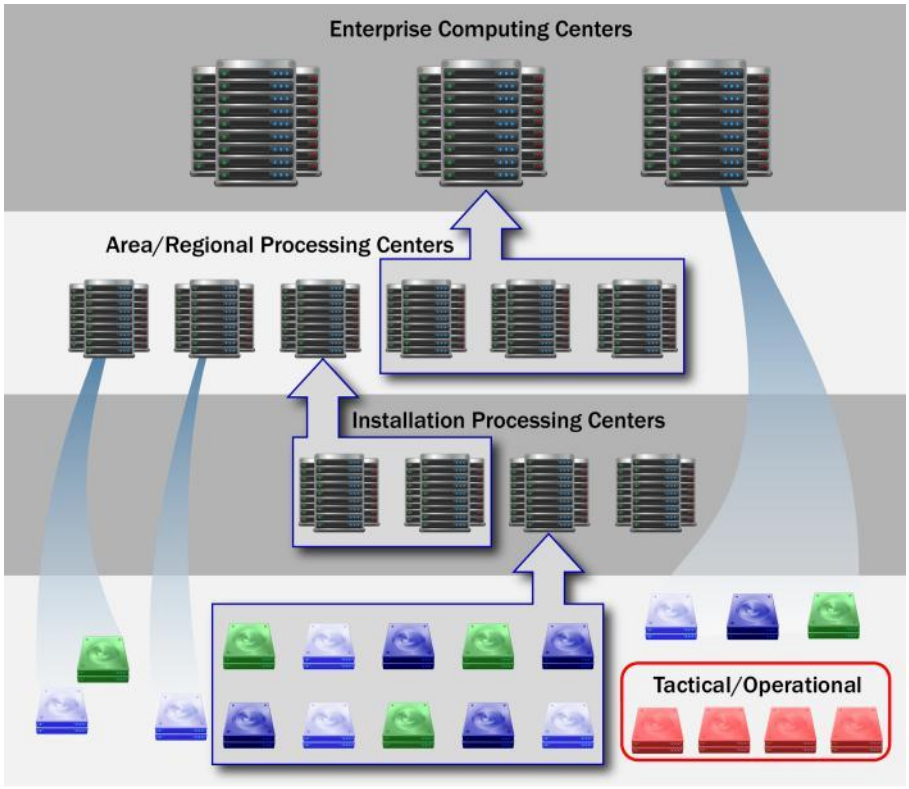

Figure 5-3: DoD Computing Center Consolidation Approach

5.1.3 End-User Services (EUS)

End-user services initiatives are focused on improving mission effectiveness and reducing costs by taking advantage of rapid changes and advances in the types of devices used to access information and applications as well as changes in the operating systems on which those systems are built. These initiatives aim to eliminate the costs of maintaining traditional workstations and the ICANs and infrastructure on which they depend, while significantly increasing end-user mobility and capability.

The consolidation efforts will create a network infrastructure that is secure, resilient, rapidly restorable, and capable of supporting multiple missions by providing the user with the mission data, interoperability, and services necessary to operate in an increasingly mobile operating environment. Next-generation end-user devices will use standardized network, data, and application services to maximize cost savings, flexibility, and defensibility. Centrally managed diversity allows for myriad interoperable devices optimized for a variety of missions and needs. The desired end state is for DoD to enjoy end-user devices that have a minimized attack surface area, enable robust network protection, and are rapidly restorable to a "known good state"; that is, they support resilience, ensure ongoing continuity of operations (COOP), and protect users' credentials. Figure 5-4 shows a notional multi-level secure desktop environment.

These initiatives set the stage for DoD to take advantage of recent and future technical changes and advances in the types of devices people use to access their information (e.g., smart phones, diskless nodes, and tablets). To take advantage of next-generation devices, DoD must move immediately to consolidate this emerging end-user infrastructure and make it "joint from birth" by taking the following actions:

1. Centrally coordinate all testing, certification, and procurement of next-generation devices at the enterprise level to reduce unnecessarily redundant testing and expenses
2. Centrally manage all next-generation device configurations and consolidate all next-generation hardware and software purchases to both take advantage of economies of scale and promote software and system reuse
3. Establish a limited number of standard DoD development platforms and repositories to reduce testing and certification costs through a "test once, use everywhere" process optimized for next-generation end-user devices with limited bandwidth
4. Coordinate continued pathfinder implementations of web-based desktop productivity software suites at the enterprise level
5. Establish technical procedures, data standards, operating protocols, memoranda of understanding, and memoranda of agreement as needed to improve interoperability and enhance information-sharing capabilities
6. Integrate voice, video, and data devices and applications

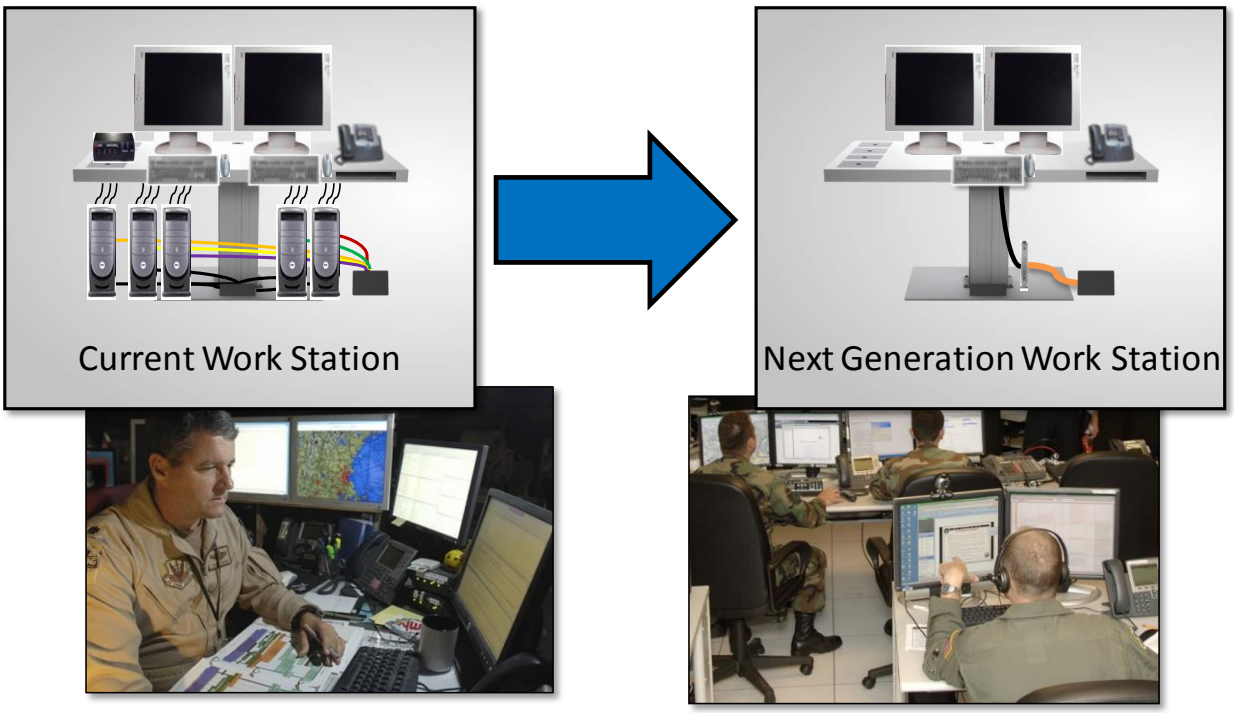

Figure 5-4: Notional Multi-Level Secure Desktop Environment[9]

5.1.4 Application and Data Services (ADS)

Application and Data Services initiatives are focused on providing secure global access to common DoD-wide solutions that enable personnel to access the people and information resources they need from any DoD computer, anywhere in the world, consistent with security classification and special access restrictions. To gain the full operational and economic benefit of the initiatives detailed in this document, DoD must change how it acquires, develops, fields, and

[9] Source: Al Udeid Combined Air and Space Operations Center (CAOC) Trusted Thin Client Training materials

maintains applications. The approach is based on developing enterprise capabilities and demonstrating that the enterprise capability is sufficiently robust to meet operational requirements. The objective is to make a compelling case that Components should not invest resources to develop, modify, or sustain capabilities comparable to the designated DoD enterprise capabilities unless there is a compelling operational need or documented business case.

DoD will pursue a four-prong approach to consolidating application and data services—

- Develop and publicize enterprise capabilities
- Publish enterprise reference architectures, including technical standards for federated enterprise solutions
- Establish a limited set of development platforms and a process for rapid incremental development, including a "tested by one, accepted by all" process for joint system certification
- Identify authoritative data sources and unnecessarily duplicative data systems

To accomplish these goals, DoD will take the following actions:

1. Develop an approach to support application development for bandwidth-constrained environments
2. Establish a limited number of standard DoD development platforms and repositories (similar to the DISA "RACE" and "Forge.Mil") to reuse government-developed code and software configurations as much as possible and thereby reduce testing and certification costs through a "test once, use everywhere" process optimized for next-generation end-user devices
3. Develop a federated enterprise solution for access control on classified and unclassified networks; this should include a suite of enterprise attribute services for personnel that includes the implementation of Component-level "Organization Servers," Global Force Management Data Initiative, and associated Defense Manpower Data Center (DMDC)- and DISA-provided services
4. Develop a federated enterprise solution for attribute-based access control on classified and unclassified networks; this should include a suite of Enterprise Attribute Services for people and devices
5. Develop a federated enterprise solution for digital signatures on classified and unclassified networks

Initial activities focus on deployment of Enterprise Messaging and Collaboration Services (including e-mail) (ADS-1) and Identity and Access Management Services (ADS-2). Identity and Access Management Services provide the foundational security capability needed for rapid and unanticipated information sharing. This managed and governed core support service provides attributes for access decisions within a centralized enterprise model. This service includes a collection of authoritative person and non-person entity (NPE) attribute data based on commonly defined and governed attributes and makes them available through an enterprise service model to integrate within DoD authorization and access capabilities (e.g., Attribute-Based Access Control).

Identity and Access Management Services provide access to identity information and can expedite both account provisioning and secure information sharing. Together with other DoD

authorization and access capabilities, the Identity and Access Management Services provide the basis for replacing time- and resource-intensive manual processes with near-real-time automated account provisioning and access control to share information resources. This core service supports a more agile, flexible, and responsive warfighting posture where the rules for access control can be quickly modified and enforced based on changing real-world conditions.

Key objectives are to—

1. Increase warfighter access to required information and services, especially across organizational and security boundaries
2. Increase network flexibility, allowing for rapid responses to operational conditions
3. Improve cyber security
4. Drive out anonymity via strong cryptographic authentication (e.g., PKI)
5. Standardize access policies to enable more consistent access decisions
6. Increase agility and interoperability by implementing commercial standards

5.1.5 IT Business Processes (BP)

The IT Business Process (BP) initiatives seek to leverage economies of scale and to improve ways of doing business to deliver IT efficiencies. The focus is to identify DoD-wide approaches to common IT business needs and direct IT-related business and operational practices that will deliver procurement, sustainment, and energy efficiencies.

DoD will build on the successes of the DoD Enterprise Software Initiative (ESI)[10] and consolidated hardware procurement approaches established by the Army and Air Force. In its first 10 years of operation, DoD ESI achieved a cost avoidance of more than $3 billion compared with General Services Administration (GSA) Federal Supply Schedule published prices.

Limiting COTS hardware and software procurements to enterprise-wide vehicles will reduce lifecycle costs by reducing both procurement expenditures and aggregate contract administration overhead costs. In addition, reducing the number of IT hardware configurations will reduce testing, patch management, and software upgrade installation costs.

Defense Business Systems account for nearly $7 billion of the annual IT budget. There are nearly 3,000 registered systems, each of which is maintained separately and operates on its own independent data store. Consolidation of these services, along with labor services, will be based on an Information Technology Infrastructure Library (ITIL) Service Catalog framework. In many cases, there will be significant cost savings associated with retiring legacy systems, halting procurement of duplicate services, and reducing the amount of redundant data maintained in duplicative systems. However, in some cases, the main benefit will be improved security and effectiveness rather than the cost reduction. Given that some systems operate on minimal budgets and lack adequate security and robustness, improving them to meet enterprise standards (especially related to security) may be cost-neutral or even require additional investment.

DoD may realize significant annual cost reductions by promoting and adopting Green IT initiatives. These initiatives focus on how DoD operates IT infrastructure; procures devices, services, and IT supplies; and consumes the resources that support IT.

[10] See http://www.esi.mil/

6 Estimated Efficiencies

The DoD CIO estimates that IT consolidation can deliver efficiencies that result in $3.2 billion to $5.2 billion over the Future Years Defense Program (FYDP). Annual efficiencies in FY16 and beyond are estimated to be between $1.3 billion and $2.2 billion per year.

In response to the SecDef-directed "zero-based review" of functions and resources, the Army identified IT efficiencies of $500 million and the Air Force identified IT efficiencies of $1.2 billion in the DoD FY12 President's Budget (PB12) submission. After subtracting Army and Air Force PB 12 budget reductions, the DoD CIO estimates that additional efficiencies of $1.5 billion to $3.5 billion over the FYDP can be obtained through future DoD enterprise consolidation efforts. Over the past several years, the Department of the Navy has consolidated its disparate networks into the largest single enterprise network in DoD, and recently established IT efficiency initiatives aligned with the consolidation initiatives outlined in this document.

Realizing these additional efficiencies will require enabling investments, as outlined in Figure 6-1. The IT consolidation initiatives will result in a combination of cost avoidance and direct and indirect budget savings. These preliminary estimates will be revised, required investments will be identified, and business case analyses will be reviewed and approved by the D, CAPE before implementation.

A significant portion of the future IT consolidation efficiencies will be the result of reduced sustainment funding for legacy capabilities that are eliminated and replaced by enterprise capabilities. Other efficiencies will be realized through reduced procurement costs or reduced energy costs.

DoD is evaluating alternative funding mechanisms and portfolio approaches for IT as part of the IT Acquisition Reform effort required by Section 804 of the 2010 National Defense Authorization Act (NDAA). These reforms will improve DoD's ability to measure IT consolidation savings.

Initiative Area	Preliminary Estimated Efficiencies ($M)*			
	Annual Efficiencies (FY2016+)		Total Efficiencies (FY2012–2016)	
	Minimum	Most Likely	Minimum	Most Likely
Computing Services	220	370	500	830
Network Services	230	730	650	1,650
End-User Services	210	230	460	570
Application and Data Services	160	240	350	710
IT Business Processes	480	700	1,530	2,100
Preliminary Estimated Total Efficiencies	1,300	2,270	3,490	5,860
Less Required Investment (FY2012–2016)	(50)	(100)	(290)	(660)
Estimated Net Efficiencies	1,250	2170	3,200	5,200
Less: PB 12 Budget Reduction				
Army	(100)	(100)	(500)	(500)
Air Force	(380)	(380)	(1,200)	(1,200)
Potential Additional Efficiencies	770	1,690	1,500	3,500

*Pending business case analysis

Figure 6-1: Preliminary IT Consolidation Efficiencies Estimates

7 Sustaining Processes

Achieving the goals and objectives of IT consolidation will require strong enterprise-level governance and monitoring led by the DoD CIO in partnership with stakeholders from across OSD and the Components, which will require substantial cultural change within the DoD decision-making community. Adherence to DoD CIO policy and Enterprise Architecture guidance must be embedded throughout DoD's core decision-making processes, and the DoD CIO must have clear, unambiguous authority across the Enterprise to hold DoD Components accountable for alignment with IT policies and initiatives and delivery of IT solutions. Strong governance mechanisms will be required both to support the consolidation efforts and to ensure that all unique operational requirements are addressed.

7.1 IT Governance

Successful consolidation of DoD's IT environment depends on principled leadership and governance. This in turn will require institutional changes in critical decision-making processes as well as a cultural reform regarding the manner in which DoD manages information and IT.

7.2 Certification and Accreditation (C&A)

To achieve IT efficiencies and deliver the promise of speed of delivery, the DoD CIO will evaluate the effectiveness of current C&A approaches. IT C&A processes may be consolidated and integrated and the number and level of autonomy of Designated Approval Authorities (DAA) may be reviewed and reduced as appropriate.

The DoD CIO will lead the effort to develop the policies and guidance necessary to consolidate DoD C&A practices, focusing on maximizing reciprocity and reducing duplicative efforts. In doing so, the DoD CIO, leading the IT Enterprise effort, will collaborate with DoD's IT Acquisition Reform Task Force to leverage the progress made on both efforts. Participation by DoD Component C&A leads will ensure that solutions are developed with input from all stakeholders.

7.3 Joint Capabilities Integration and Development System (JCIDS)

The JROC, chaired by the Vice Chairman of the Joint Chiefs of Staff, is DoD's governing body for identifying, approving, and validating the capability gaps and requirements identified by Warfighting, Intelligence, Business, and Enterprise Information Environment (EIE) mission area managers. A hierarchy of boards, including the Joint Capabilities Board (JCB) and Functional Capabilities Board (FCB), along with the processes delineated in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170, supports the JROC in this capacity. The DoD CIO will recommend changes to the JCB and FCB approach to streamline EIE requirements and prioritize capability delivery. In addition, DoD recommends the following JCIDS-related actions to ensure compliance with EIE requirements:

- **Modify JCIDS Documentation (CJCSI 3170 series)** to require documentation of compliance with the DoD Information Enterprise Architecture (IEA) that contains business rules and relevant reference architectures that apply to all IT investments
- **Modify Interoperability Instruction (CJCSI 6212**) to strengthen DoD IEA compliance, clarify the Net-Ready Key Performance Parameter with respect to the DoD IEA, establish the requirement to align and comply with relevant reference architectures, and require adoption of the Enhanced Information Support Plan (EISP) process to assess compliance

- **Modify the Business Capability Lifecycle (BCL) process** to require DoD IEA compliance

7.4 Planning, Programming, Budgeting, and Execution (PPBE)

IT consolidation may require changes to Components' budget and expenditure plans. As these changes are understood, the DoD CIO will—

- Submit input to and participate in developing the Defense Planning and Programming Guidance (DPPG)
- Participate in front end assessments as deemed appropriate by the SecDef
- Participate in the program and budget review by submitting issue papers or change proposals that recommend DoD continue, modify, terminate, or initiate funding for EIE projects/programs, participate in all program review decision-making forums (e.g., issue teams, 3-Star Programmers, DAWG), and provide the Comptroller with all information required for budget review decisions

In addition, the DoD CIO will review DoD's spending on IT programs in coordination with D, CAPE and the comptroller and recommend adjustments based on that review.

7.5 Defense Acquisition System (DAS)

Contracting officers, program managers, and other acquisition professionals are constrained by Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) with respect to ensuring all IT procured by DoD fully meets, but does not unnecessarily exceed at additional cost, all validated requirements for the subject procurement action. In the majority of cases, "validated requirements" are not determined via the JCIDS process, but rather by local requirements generators who may or may not be familiar with, or feel compelled to use, enterprise capabilities (e.g., data centers, networks, enterprise services). DoD acquisition and procurement policy and processes, as well as relevant DFARS clauses, if possible, must be modified to direct contracting officers to ensure that all DoD IT contracts require the use of, and prohibit the duplication of, enterprise capabilities.

Successful IT consolidation will require DoD to establish a common set of DoD EIE acquisition and procurement strategies. Although technical standards achieve a level of interoperability, the next phases of the consolidation effort cannot be accomplished unless the acquisition and procurement strategies are synchronized across all Components.

The DoD CIO recommends the following actions to ensure DoD IT policy and guidance is followed throughout the DAS process:

- Change DoD Directive (DoDD) 5000.01, "The Defense Acquisition System" and the Business Capability Lifecycle to enforce compliance with DoD IEA and the use of available enterprise capabilities within major acquisition activities.
- Develop and institute a standard contract clause, to be inserted in all acquisition strategies and contracts for DoD IT goods and services, requiring compliance with the DoD IEA, and the use and non-duplication of designated enterprise capabilities.
- Incorporate the IA requirements and procedures currently defined by the DoD Information Assurance Certification and Accreditation Process (DIACAP) into the DAS processes to ensure effective IA capabilities are designed into all IT systems, from concept through systems engineering. This applies equally to the acquisition and

procurement of IT capabilities that traditionally fall below the threshold criteria for formal acquisition.

Appendix A Network Services Initiatives

NS1–Consolidate Security Infrastructure

Multiple generations of Top Level Architectures (TLA) provide network perimeter security across DoD. In many cases, the equipment used is nearing the end of useful life, requiring both refresh and new technology for continuing defense of the network and providing enhanced capabilities for protecting against emerging threats. This initiative is to design and deploy a DoD Enterprise-Top Level Architecture (D-TLA) that standardizes equipment, improves IA security capabilities, reduces the number of DISA point-of-presence (PoP) connections, and simplifies systems management.

NS2–Consolidate NetOps Centers

NS2 involves migrating from the numerous separate Component NetOps centers to joint NetOps centers that align with common processes and standards, select and adopt common tools, and automate network incident response capabilities. This will leverage buying power for enterprise-wide network operations software and licenses and centralize hosting of network operations services in DoD computing centers, thus reducing hardware costs and improving security (Under review by USCYBERCOM).

NS3–Implement Cross-Domain Solution as an Enterprise Service

This effort to create enterprise application services that are “cross-domain enabled” Involves engineering and deploying comprehensive, enterprise-grade services for common key applications such as e-mail, machine-to-machine data transfer, portal synchronization, chat, and web services. This effort aims to provide reliable, secure, well-defended standard services for the COTS application data formats that make up the bulk of cross-domain requirements. These COTS data formats, such as Simple Mail Transfer Protocol (SMTP) e-mail, Microsoft Office documents, and .pdf files, are predictable, well understood, standard, and common. The goal is to make it an easy investment and risk decision for a DoD organization to use the provided enterprise service rather than to engineer, staff, and defend a local solution.

NS4–Implement Standard Certification and Accreditation Process

For DoD to fully transition to the new harmonized guidance, it plans to first revise its existing 8500 series of guidance. This includes revising the information security policy documented in DoDD 8500.01 and in DoD Instruction (DoDI) 8500.2, the C&A process contained in DoDI 8510.01, as well as various additional instructions and guidance. The first major step is to release the revised DoDD 8500.01 and DoDIs 8500.2 and 8510.01. After this occurs, DoD plans to develop additional implementation and assessment guidance, technical instructions, and other information. The release dates for these additional items have not yet been established because their development or revision depends on the final publication of revisions to the 8500 series guidance.

NS5–Extend Joint Networks Over SATCOM

Extending joint networks over Satellite Communications (SATCOM) provides an affordable, DoD Enterprise worldwide SATCOM Gateway capability by centralizing and unifying

management and control, budget, investment, and lifecycle management; and by reducing duplication.

NS6–Implement Video over IP as an Enterprise Service

The current Defense Information Systems Network (DISN) Video Services–Global (DVS-G) Network provides both Secret Internet Protocol Router (SIPR), Internet Protocol (IP), and Integrated Services Digital Network (ISDN) access for video services. This is a non-government contracted service that is based on minutes of utilization in the continental United States (CONUS) and on fixed rates for outside continental United States (OCONUS) locations. Network Services is developing, in coordination with industry, the architecture for the next generation of Enterprise Video IP services for both the SIPR and the Unclassified but Sensitive Internet Protocol Router (NIPR). The Enterprise Video IP is leveraging Secure Internet Protocol (SIP) with a migration path to Assured Services-SIP for a highly available and quality video service. Concurrent with deployment of Video over IP as an Enterprise Service, the Services and Agencies will turn off and decommission all multipoint control units (MCU), video hubs, and related infrastructure.

NS7–Implement Voice over IP as an Enterprise Service

The current Voice Systems Network provides global unclassified (DSN) and classified (Voice over SIP and DRSN) voice services. These are voice services provided on DISN in CONUS and OCONUS locations. Network Services is developing, in coordination with industry, the architecture for Enterprise Voice over Internet Protocol (VoIP) Services to provide a full range of voice-related capabilities to more than 4 million DoD users from a central location that fully leverages the DISN and IP technologies. The Enterprise VoIP is leveraging Assured Services-SIP with quality of service for a highly reliable, available, and survivable voice service. This approach will eliminate the duplication of costs for voice services, O&M, network operations, sustainment, and IA at nearly 2,000 locations worldwide. It also allows for improved security and the rapid phase-in of a full suite of unified capabilities with collaboration, conferencing, mobility, and portability features to improve DoD end-to-end information dominance for both fixed and tactical (deployable) missions at a lower total cost of ownership.

NS8–Transport Joint Enterprise Network (JEN)

The GIG 2.0 provides a vision of a single, secure information environment which will be realized through the Joint Information Environment (JIE). As a specific use case, the Joint Enterprise Network (JEN) has been proposed as a consolidated, secure, robust, and standards-based IT infrastructure that leverages a joint governance framework. In supporting United States Africa Command (USAFRICOM) and United States European Command (USEUCOM) missions, the JEN will provide operational net-centric enterprise services, consolidated IT service support, a common NetOps architecture, and redundant transport and connectivity for classified secret, unclassified, and non-classified information systems (IS). The JEN is designed to meet DoD and NSA requirements while maximizing utilization of DoD IT investments in a given region without compromising security. This is accomplished by using virtualization technologies, ultimately allowing multiple organizations to leverage and access standardized net-centric services, while affording some policy deviation to meet unique mission requirements. The JEN project also supports telecommunication consolidation and will provide the region with the opportunity to integrate and collapse approximately 50 Army sites into the DISN theater infrastructure. Telecommunications sustainment, technology refresh, and operational support

staff will be removed or eliminated for the U.S. Army in Europe. The project will be developed to support Enterprise Data Center Consolidation efforts and to provide services to the warfighter, in both garrison and tactical environments, throughout all phases of joint operations. Similar efforts are underway in Korea.

NS9–Enterprise Network Infrastructure Reliability

This initiative upgrades the DISN to support a 99.997% operational availability at all Joint Staff–validated locations using upgraded diversity, maintenance response capabilities, satellite/wireless fly-away, and extensions to the edge via innovative range-extension capabilities. Current DISN sustainment funding achieves a 99.5% operational availability. This level of operational availability cannot support enterprise voice, enterprise e-mail, enterprise thin client, and other enterprise information and communications technology efficiencies. This initiative is a cost center that makes the other initiatives operationally viable for DoD and Intelligence Community (IC) needs.

NS10–Defense Red Switch Network (DRSN) Rationalization

The DRSN supports critical C2 secure voice capabilities, and implementation of a DRSN switch system for a command requires that the Joint Staff approve a validated requirement through the CJCSI process. DRSN switches support a number of critical capabilities, the three most critical are: 1) the large conferencing and conferencing management capability; 2) the ability to support calls and conferences involving various security levels (Secret to Top Secret/Sensitive Compartmented Information); and 3) gateway functions (interfaces) to other secure voice systems. Recent guidance from the SecDef to support cost reductions precipitated the review and analysis of the DRSN and a consideration for potentially reducing the number of switches in the DRSN. Currently, there is no other product available that can perform the critical capabilities of the Raytheon DRSN switch, but the number of switches potentially could be reduced by reevaluating requirements and determining if replacing them with VoSIP and/or consolidating service at some location would still satisfy operational requirements.

Appendix B Computing Services Initiatives

CS1–Data Center and Server Consolidation

Data Center and Server Consolidation focuses on reducing the overall cost of DoD data and computing center operations and energy consumption while sustaining or increasing mission effectiveness. Most DoD Components have planned or already are consolidating data and computing centers in accordance with the OMB-directed Federal Data Center Consolidation Initiative (FDCCI). The FDCCI directed a reduction in data centers primarily through the use of virtualization techniques and leveraging cloud computing. DoD's current assessment is that it can achieve a 30% (+/-) decrease in data/computing centers, rack space, and servers.

CS2–Computing Infrastructure and Services Optimization

The IT infrastructure of individual installations is composed of multiple networks and IT service provider organizations, resulting in duplicative investments, redundant processes, and conflicting policies. This initiative optimizes IT infrastructure and services through consolidation and increased sharing, in alignment with COCOM operations plans, and by leveraging IT service management best practices. This initiative will improve end-users' experience by simplifying IT policies and processes; consolidate and commoditize disparate IT services for improved agility in response to dynamic information requirements; improve interoperability for better information sharing; reduce manpower, training, hardware, software, and O&M costs; and align with IT service management industry best practices.

CS3–Cloud Computing

This initiative moves computing services into the cloud with the objectives of improving information security, reducing infrastructure costs, and enabling rapid discovery and use of new net-centric capabilities. It targets the migration of the development environment into the cloud through Forge.mil, Rapid Access Computing Environment (RACE), and other designated activities. Forge.mil enables the collaborative development and use of open-source and DoD community source software. RACE uses cloud computing technology to provide development platforms quickly, inexpensively, and securely. This initiative accelerates the fielding of services for secure and rapid information sharing and enables developers to deliver software more rapidly. It includes capabilities such as "Storefront" and "Marketplace" to provide user access portals for rapid discovery and use of cloud-hosted applications.

CS4–Service Desk Consolidation and Optimization

DoD operates hundreds, if not thousands, of individual help desks, which costs millions of dollars to staff, operate, and maintain. Each individual help desk, for the most part, conducts its functions in a similar manner. The purpose of the Service Desk Consolidation initiative is to consolidate the assortment of installation-level and organization-level help desks into a DoD Service-level Enterprise Help, or "Service" Desk (e.g., Army-level, Navy-level), with the ultimate goal of consolidating into a DoD-level Service Desk provided from the DoD cloud. Establishing consolidated Enterprise Service Desks for each of the COCOMs, DoD Services, and agencies, leveraging industry best practices and shared IT infrastructure, will result in hundreds of millions of dollars in savings across DoD by eliminating redundant services and capabilities.

More important, consolidating help desks will provide end users with better and more consistent and repeatable service.

Appendix C Application and Data Services Initiatives

ADS1–Enterprise Messaging & Collaboration Services (including E-mail)

Current DoD messaging and collaboration capabilities consist of multiple disparate services developed and managed in a stove-piped manner. Consequently, these services face numerous shortcomings to include requiring cumbersome migrations when users change organizations; lack of permanent identity presence; inability to view a global address and contact list that covers all MilDeps and Components; inefficient search capabilities; and the lack of an integrated e-message platform. Additionally, services providing different collaboration methods are not designed to be interoperable and complimentary to each other. Unified Communications & Collaboration (UC&C) will address these limitations by providing location independent capabilities, to include IM/Chat, Email, Portal, and web conferencing, that enable information sharing from any device attached to a DoD network.

ADS2–Identity and Access Management Services

Identity and Access Management Services collect and provide common identity attributes for people, organizations, and other non-person entities (e.g., files and devices on a network). Identity attributes (e.g., U.S. citizenship, clearance, employee type) are used to enable access decisions and provide information to Attribute-Based Access Control (ABAC) capabilities in a secure, consistent fashion. Identity and Access Management Services provide a foundational security capability that is needed for rapid and unanticipated information sharing. Together with other DoD authorization and access capabilities, these services provide the basis for replacing manually intensive processes with automated account provisioning and for controlling access to shared information resources in near real time. These services support an agile, flexible, and responsive warfighting posture where the rules for access control can be quickly modified and enforced based on changing real-world conditions.

ADS3–Enterprise Services

This initiative provides a common platform for discovery, asset management, deployment, engineering, and sustainment of enterprise applications and data services. It enables a scalable infrastructure (e.g., the DISA RACE) to leverage a common security and access control framework that will reduce the number of unique interfaces required for access to applications and data repositories; reduce costs associated with developing and maintaining multiple services; provide a common infrastructure capability that better enables Services and Components to locate, access, and use shared services; and reduce duplicative and under-used devices and associated licenses, support, and utilities costs.

ADS4–Records Management

This initiative provides common records management functions available across the DoD Enterprise where official DoD records types are categorized (including versioning and tagging), archived, and stored for later search and retrieval. This initiative supports a streamlined capability to respond to requests for federal records, Freedom of Information Act (FOIA) cases, Equal Employment Opportunity (EEO) cases, and e-discovery litigation holds.

Appendix D End User Computing Services Initiatives

EUS1–Next-Generation End-User Devices

A significant number of DoD personnel work in non-deployable offices performing tasks for which they need only basic office automation software on NIPRNet-attached desktop or notebook computers. These users can be rapidly transitioned to next-generation devices and web-based software, which could be fielded, operated, and maintained at a fraction of the cost of the existing desktop and notebook computers. Next-generation devices would require little or no local storage and would use web-based versions of common applications (e.g., word processing, slide presentation, spreadsheet, e-mail). In addition to cost savings, this migration would dramatically increase the security and resilience of DoD networks. Next-generation end-user devices will use standardized network, data, and application services to maximize cost savings, flexibility, and defensibility. Such devices have a minimized attack surface area, enable robust network protection, and are rapidly restorable to a "known good state"; that is, they support resilience, ensure ongoing continuity of operations (COOP), and protect users' credentials.

EUS2–Multi-Level Security Domain Thin-Client Solutions

This initiative involves transitioning the DoD multi-classification end-user community to a virtualized desktop environment, where next-generation devices replace the heavy desktop computers used in classified, multi-fabric environments. Migrating multi-fabric users to a virtualized desktop environment will significantly increase cross-domain efficiencies and effectiveness by reducing operating cost, improving security, enhancing COOP, and facilitating telecommuting. This initiative eliminates the need for users to have multiple workstations at their desk and to constantly switch desktops to work across various domains. Savings would be achieved by eliminating the costs associated with maintaining multiple ICANs for classified computing and the costs associated with patching, securing, and managing three or more desktop computers per classified user.

EUS3–Interoperability Within DoD and Between Mission Partners

This initiative involves developing and implementing a DoD Enterprise Framework that provides the standards, guidance, architecture, and CONOPS to enable a cohesive approach to interoperability between DoD and its mission partners. The DoD Enterprise Framework will identify and eliminate redundant, duplicative, and overlapping investments in DoD and mission partner standards. These standards include governance, accountability, and enforcement, technical procedures, and data standards (e.g., master data, standard identifiers, naming conventions, schemas, interface specifications, and characteristics). DoD will team with mission partners to achieve efficiencies and ROIs through agreed-on practices that will enable flexible Identity and Access Management and minimize security risks while providing for maximum interoperability and data sharing. A focus on web-based enterprise applications and capabilities will further enhance data sharing and the speed of information to the end user.

Appendix E IT Business Process Initiatives

BP1–Consolidate Software Purchasing

This initiative involves centrally funding and managing DoD-wide enterprise licenses for the most widely used commercial software through the DoD Enterprise Software Initiative (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. This initiative will focus on discrete brand names and prohibit the purchase of any software application that is available through the DoD ESI from any other source without a DoD CIO–approved waiver. This action will reduce lifecycle costs by reducing procurement expenditures, easing patching and maintenance, and reducing aggregate contract administration overhead.

BP2–Consolidate Hardware Purchasing

This initiative will drive procurement of all DoD commodity IT hardware (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), the Marine Corps Hardware Suite (MCHS), and the Marine Corps Enterprise Licensing Management System (MCSELMS). DoD will modify these processes to ensure capture of other Components' basic configuration requirements. This initiative also may adopt other Component IT hardware buying processes or establish new vehicles to ensure coverage of other IT hardware devices. DoD will prohibit purchase of these IT hardware items from any source other than these vehicles. This action will reduce lifecycle costs by reducing procurement expenditures, easing testing and maintenance support tasks, reducing aggregate contract administration overhead, and using "green" specifications to reduce power consumption.

BP3–Optimize IT Services Purchasing

This initiative will provide centrally managed IT service contracts, including IT infrastructure, to drive lower procurement costs and develop common standards for delivery orders. DoD will prohibit the purchase of IT services for any of the expanded DoD ITIL service categories from any other source without a DoD CIO–approved waiver. DoD will adopt existing government IT service acquisition vehicles that meet the common standards and will establish new DoD acquisition vehicles to meet expanded DoD ITIL service requirements that cannot otherwise be fulfilled. By centralizing management of the IT services acquisition portfolio and streamlining the acquisition of IT services, DoD will realize cost savings by reducing contracting overhead, ensuring best practices are available and used, and educating the IT acquisition workforce.

BP4–Common Business Process Foundation

The focus of this initiative is to support standardizing DoD-wide common business processes through shared applications. Currently, there are nearly 3,000 registered IT business systems within DoD, representing a $7 billion annual expense. Many of these systems are maintained separately and operate their own independent IT infrastructure. The near-term focus of this initiative is to select existing applications that meet the desired criteria and designate them as interim Core Enterprise Business Services that will be mandated for use across all DoD Components as the standard for performing these common business processes.

BP5–Promote and Adopt "Green" IT

Through this initiative to promote and adopt "green" IT activities, DoD may be able to realize annual cost reduction/avoidance estimated at more than $300 million. These activities focus on how DoD operates IT infrastructure; buys devices, services, and IT supplies; and consumes the resources that support IT. Green IT activities reduce DoD's power consumption and dollars spent on energy (IT energy footprint) while also reducing carbon emissions and waste generated (environmental footprint). Recommendations for activities to implement will be based on industry best practices and Federal Government and DoD analyses. Three sets of activities to be executed in a 3-year cycle include, but are not limited to: (1) aligning ESI with DoD's Green Procurement Program Strategy, Electronics Stewardship Implementation Plan, and Strategic Sustainability Performance Plan; (2) designing, consolidating, and operating data centers and hosting services in a manner consistent with the commercial best practices of adopting new energy-efficiency technologies and practices; and (3) replacing inefficient end-user devices with those that meet the Energy Star 5.0 specification.

Appendix F Acronym List

ABAC	Attribute-Based Access Control
ADS	Application and Data Services
AoA	Analysis of Alternatives
AOR	Area of Responsibility
A/RPC	Area/Regional Processing Centers
AT&L	Acquisition Technology and Logistics
BCA	Business Case Analysis
BCL	Business Capability Lifecycle
BP	Business Process
C&A	Certification and Accreditation
C2	Command and Control
CAPE	Cost Assessment and Program Evaluation
CB	Consolidated Buy
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COA	Course of Action
COCOM	Combatant Command
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COTS	Commercial Off-the-Shelf
CS	Computing Services
DAA	Designated Approval Authority
DAS	Defense Acquisition System
DAWG	Deputy's Advisory Working Group
DBSMC	Defense Business Systems Management Committee
D, CAPE	Director–Cost Analysis and Program Evaluation
DCMO	Deputy Chief Management Officer
DFARS	Defense Federal Acquisition Regulation Supplement
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoD IEA	DoD Information Enterprise Architecture
DoD ITIL	Department of Defense Information Technology Infrastructure Library
DPPG	Defense Policy and Planning Guidance
DRSN	Defense Red Switch Network
D-TLA	DoD Enterprise–Top Level Architecture
DVS-G	DISN Video Services–Global
ECC	Enterprise Computing Center
EEO	Equal Employment Opportunity
EIE	Enterprise Information Environment
EIE FCB	Enterprise Information Environment Functional Capability Board

ESI	Enterprise Software Initiative
EUS	End-User Services
FAR	Federal Acquisition Regulation
FCB	Functional Capabilities Board
FDCCI	Federal Data Center Consolidation Initiative
FEA	Front End Assessment
FMR	Financial Management Regulation
FOIA	Freedom of Information Act
FY	Fiscal Year
FYDP	Future Years Defense Program
GIG	Global Information Grid
GSA	U.S. General Services Administration
IA	Information Assurance
IC	Intelligence Community
ICAN	Installation Campus Area Networks
ICD	Initial Capabilities Document
IP	Internet Protocol
IPC	Installation Processing Center
ISDN	Integrated Services Digital Network
IT	Information Technology
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Force Commander
JIC	Joint Integrating Concept
JIE	Joint Information Environment
JOpsC	Joint Operations Concepts
JP	Joint Publication
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JS	Joint Staff
JTF	Joint Task Force
JUON	Joint Urgent Operational Needs Process
LMR	Land Mobile Radio
MCHS	Marine Corps Hardware Suite
MCSELMS	Marine Corps Enterprise Licensing Management System
MCU	Multipoint Control Unit
MDAP	Major Defense Acquisition Program
MilDeps	Military Department
NDAA	National Defense Authorization Act
NetOps	Network Operations
NIPR	Unclassified but Sensitive Internet Protocol Router
NPE	Non-Person Entity
NS	Network Services
NSA	National Security Agency
NSS	National Security System
OCONUS	Outside Continental United States
OMB	Office of Management and Budget

OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PB	President's Budget
PDR	Preliminary Design Reviews
PKI	Public Key Infrastructure
POM	Program Objective Memorandum
PoP	Point-of-Presence
PPBE	Planning, Programming, Budgeting, and Execution
QEB	Quarterly Enterprise Buy
RACE	Rapid Access Computing Environment
ROM	Rough Order of Magnitude
ROMO	Range of Military Operations
SATCOM	Satellite Communications
SDN	Service Delivery Node
SecDef	Secretary of Defense
SIP	Secure Internet Protocol
SIPR	Secret Internet Protocol Router
SMTP	Simple Mail Transfer Protocol
TLA	Top Level Architecture
TS/SCI	Top Secret/Sensitive Compartmented Information
USAFRICOM	United States Africa Command
USCYBERCOM	United States Cyber Command
USD	Under Secretary of Defense
USD(C)	Under Secretary of Defense (Comptroller)
USD(P)	Under Secretary of Defense (Policy)
USEUCOM	United States European Command
USSTRATCOM	United States Strategic Command
VoIP	Voice over Internet Protocol

This page intentionally left blank.