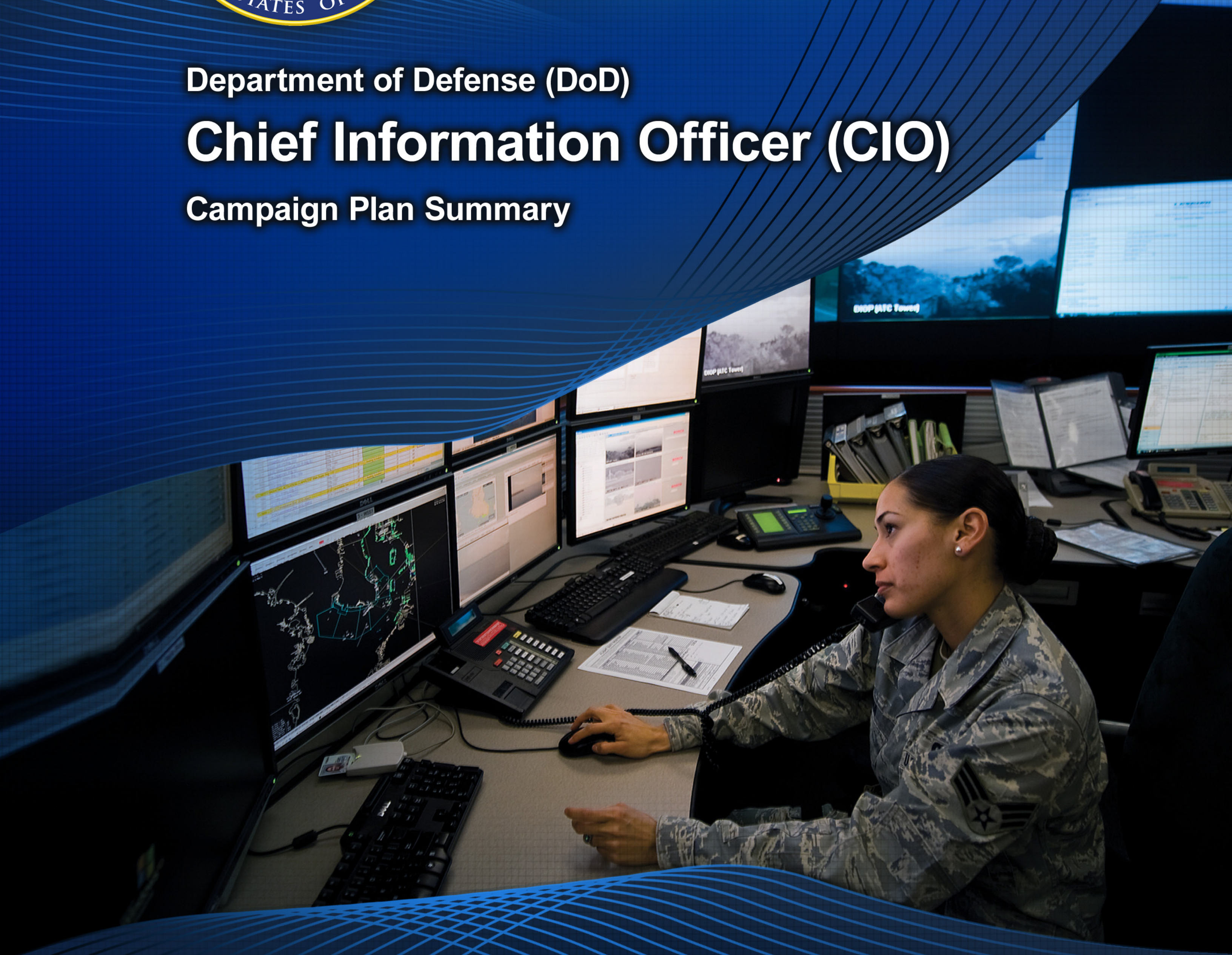
Department of Defense (DoD)

Chief Information Officer (CIO)

Campaign Plan Summary



FROM THE DOD CIO

The challenge of managing information technology (IT) within the Department of Defense has never been greater. The Department's mission continues to expand to encompass military, peacekeeper, and disaster relief operations across the globe. At the same time, the unprecedented growth and availability of new information technologies adds tremendous complexity to the choices available. With these new capabilities come new challenges to the security of our environment. These challenges must be met in an environment of significant resource constraints and declining budgets.

At the same time, the opportunity has never been greater. Increasingly, mission success depends upon the ability of our military commanders and civilian leaders to act quickly and effectively—in concert with multiple mission partners—based on the best, most accurate, and timely information available. It is our job to provide the information environment they need to accomplish this. In addition, our workforce is eager to apply the powerful collaboration tools and practices they routinely use in their personal lives. We must enable this powerful set of capabilities as rapidly as possible, without compromising safety and security.

The DoD CIO team drives the evolution of DoD's network and information capabilities to meet the ever changing mission needs of the Department. In partnerships that include Defense Information Systems Agency (DISA), the National Security Agency (NSA), United States Cyber Command (USCYBERCOM), the Military Departments (MilDeps), and the Intelligence Community, we are developing and implementing enterprise-wide approaches to improve service delivery and security—and realize savings—through network optimization. We are working to achieve a future DoD network vision of seamless, secure information sharing across all parts of the Department and with all mission partners.

The Campaign Plan lays out areas of execution, strategic objectives, priorities, actions, and tasks that the DoD CIO team is pursuing to move the Department toward this vision. It reflects the full scope of activities being performed across the DoD CIO organization. It identifies a set of commitments to which we will be held accountable, while at the same time representing enterprise direction around which our partners in the services and agencies can align their activities.

A seamless, secure information environment is critical to the Department's success. Everyone within the Department (and across our mission partners) has a stake in this challenge. I invite you to join me in working collaboratively to deliver the essential capabilities presented in the plan. *Together, we will strengthen the DoD by delivering the agile and secure information capabilities needed to enhance our nation's combat power and decision making.*

Teresa M. Takai, DoD CIO

PART I

This brochure provides a summary, in two parts, of the DoD CIO's Campaign Plan released on October 5, 2011.

Part I provides the DoD CIO's perspective on the significance of the work covered by the Campaign Plan and addresses topics influencing that work. Topics include guiding principles for the development and execution of the Campaign Plan, the DoD CIO's Vision and Mission, and challenges facing the DoD CIO and the Department as a whole. Part I also discusses the partnerships necessary to address those challenges, the DoD CIO's technology leadership role, alignment to DoD mission priorities, and the organization and execution of the Campaign Plan.

GUIDING PRINCIPLES FOR DEVELOPMENT AND EXECUTION OF THE DOD CIO CAMPAIGN PLAN

- Lead the DoD Information Enterprise.
- Deliver timely, relevant solutions to satisfy warfighter needs through incremental capability improvements/ deployments.
- Establish clear objectives and deliverables to enable internal DoD CIO prioritization and focus in achieving capabilities and mission outcomes.
- Incentivize and encourage DoD Component initiatives that contribute to the overall DoD IE.
- Collaborate across the DoD and interagency using early and consistent engagements to drive IT initiatives that enhance mission performance and align to DoD CIO objectives.

THE DOD CIO VISION AND MISSION

The DoD CIO is the Principal Staff Assistant (PSA) and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control; communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology, including National Security Systems (NSS); information resources management (IRM); spectrum management; network operations; information systems; information assurance; positioning, navigation, and timing (PNT) policy; sensitive information integration; and contingency support and migration planning. The DoD CIO is tasked with improving the combat power of the Department—as well as its security and efficiency—by ensuring that the Department treats information as a strategic asset and that innovative information capabilities are available throughout all areas of DoD supporting warfighting, business, and intelligence missions.

VISION

DoD and partners securely access information and services they need at the time, place and on approved devices of their choosing.

MISSION

We lead the DoD Information Enterprise by defining a shared vision, setting overall policy, and driving the standard for the information infrastructure that supports Warfighting, business, and intelligence missions.

To accomplish the mission, the DoD CIO:

- Works with key stakeholders across the Department to ensure that mission-critical information is visible, accessible, and understandable to all authorized users in a trusted environment without regard to location or time.
- As PSA, leads specific IRM capabilities including command and control (C2), communications, IT infrastructure, and information assurance (IA), ensuring that these capabilities are architected, engineered, and delivered in a manner that optimizes the Department's mission capabilities, increases the Department's security posture, and makes most effective use of the Department's financial resources.
- Leads DoD's network cybersecurity/information assurance efforts and manages enterprise information sharing risks, while at the same time protecting our information assets.
- Supervises overall operation and defense of the DoD Information Enterprise.

CHALLENGES

The DoD CIO faces a wide range of challenges, including: enabling efficiencies; providing cybersecurity; facilitating agile, effective information and PNT capabilities; and adapting to an ever-changing technological landscape while leading the Department in thinking and acting like an enterprise.

To gain efficiencies, the Department must aggressively transition from single threaded mission support capabilities managed by hundreds of organizations spread across the globe to enterprise level capabilities. The Department must transform IT solutions, deployments, and operations to Enterprise IT Services, and establish them as on-demand services that are scalable, diverse, and offered as a managed package to support every need within the DoD. DoD must concurrently streamline the slow, cumbersome processes by which information capabilities are conceived, acquired, secured, and delivered. Moreover, given the constraints of declining budgets, we must also make hard decisions on which investments to fund.

The DoD CIO must also address the growing cybersecurity challenge. As DoD becomes more dependent on information capabilities, our adversaries are even more motivated to see our information, subvert our command and control channels, and deny us use of our information and communications infrastructure. Since our adversaries are quick to react whenever the Department deploys new defensive postures, we must always focus on enhancing our cybersecurity posture. There will never be a time that we can assume a “comfort” posture.

Our people across the globe—warfighters, decision makers, and those in support roles—demand broader and more timely access to information to better perform their missions. Therefore, the DoD CIO must address this challenge by providing the advocacy and guidance necessary to facilitate agile, rapid delivery of effective, secure information capabilities across all missions and functions. These capabilities must leverage the best IT available (across a range of technologies, such as mobile end user devices, networks, services, systems, and applications) to support the increased, ever evolving information demands of our users, both at home and in theater. Additionally, since network barriers affect our ability to effectively and securely share information and complete our mission, the DoD CIO must proactively work to remove barriers to network access and information sharing within the Department and between DoD and its mission partners.

To meet these challenges, the DoD CIO must lead the Department in thinking and acting as a single enterprise, rather than a set of discrete organizations. To achieve this “enterprise thinking,” the DoD CIO must work collaboratively with key leaders and stakeholders to develop DoD-wide strategies to achieve unity of purpose; champion enterprise capabilities where appropriate; and establish strong but lean governance to ensure that our information capabilities are interoperable across DoD and with our mission partners.

COMPARISON OF CURRENT AND FUTURE STATE

CURRENT STATE	FUTURE STATE
• Focus on IT systems	• Focus on IT services
• Delivery of complete major IT systems	• Incremental development and fielding
• Component or sub-Component level solutions	• Common DoD-wide solutions
• Certification and Accreditation (C&A) at sub-Component or individual organization level, without reciprocity	• Enterprise-wide C&A reciprocity
• Duplication of capabilities caused by Component or sub-Component-centric network approach	• Enterprise-wide capabilities eliminate unnecessary duplication of capabilities
• Organizationally-specific standards inhibit interoperability	• DoD-wide standards promote interoperability
• Unique Component and sub-Component NetOps environments underutilize resources and make operating the network inefficient, ineffective, and less secure	• Consolidated NetOps environment provides greater efficiency, effectiveness, and security due to centrally managed architectures, standards, and standardized joint processes
• NetOps visibility of information assets limited to Component or sub-Component level, resulting in inefficient usage	• Global NetOps visibility of information assets enables dynamic reallocation to meet shifting operational demand
• Data center standards are optimized at the individual Component or sub-Component level	• Enterprise data centers operate according to enterprise standards, enabling reduction in the number of data centers
• Lack of security mechanisms requires DoD and mission partners to build unique infrastructure, for each coalition, to enable information access	• Enterprise security mechanisms enable secure connection and control across mission partner network boundaries
• Network attacks are handled in reactive mode and require a forensic approach to identify the attacker	• Data and networks are architected to anticipate attacks, so that penetrations are easy to spot and damage is easy to contain
• Access to information based on location and organization	• Access to information based on who you are and your information needs
• Individual sign-on for each system and site	• Single sign-on
• User IT experience is greatly different from pre-deployment to deployment	• Forces find similar IT experience between pre-deployment and deployment
• Disruptions in access during reassignment	• Minimal disruption during reassignment
• Combatant Command (COCOM)-specific C2 solutions	• Enterprise-wide C2 solutions

SUCCESS THROUGH PARTNERSHIPS

Given the many challenges DoD faces in this evolving environment, the DoD CIO must work closely with partners both internal and external to the Department. Together, we must develop shared approaches for implementing, maintaining, and securing the capabilities, services, and products that support the full spectrum of operations.

Chief among these partnerships is the leadership level network and services partnership forged between the DoD CIO, DISA, NSA, and USCYBERCOM. As DoD moves forward, this partnership will move beyond oversight of the core capabilities that DISA and USCYBERCOM own and operate. In the future, this partnership will provide vision, policy, standards, and engineering expertise in the form of unified guidance to all DoD Components, across all networks and infrastructure services.

The next tier of this relationship is the network and services management partnership forged between the DoD CIO, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), and DoD Components (especially DISA, NSA, USCYBERCOM, and the MilDeps). This strong, collaborative partnership capitalizes on the unique strengths of each partner to provide the foundation to acquire, build, and secure our networks. The DoD CIO provides information resources policy and USD(AT&L) provides acquisition policy and program oversight functions, while DISA and other DoD Components focus on acquiring, building, and securing our networks and services. In the operational side of this partnership, the DoD CIO works with USCYBERCOM to provide oversight functions to all DoD organizations that operate and defend DoD networks.

The DoD CIO also has established an information capability delivery partnership with the DoD Components (especially DISA, NSA, USCYBERCOM, and the MilDep CIOs), other Office of the Secretary of Defense (OSD) staff elements, as well as the Joint Chiefs of Staff. These organizations work together across all information capabilities and management functions (not just networks and services) to leverage the three major decision processes of the Department (requirements, budget, and acquisition) to determine the capabilities needed; plan and budget the necessary resources; acquire them in the most cost-effective and efficient manner possible; and ensure they are delivered in a trusted, secure way. This partnership also integrates the policies and processes by which the Department generates, shares, protects, and defends information assets that drive their functions across the DoD.

Additionally, the DoD CIO has a cyber-workforce development partnership collaborating with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and DoD Components to establish policies and procedures to hire, train, and retain the diverse group of IT professionals needed to engineer, acquire, build, operate, and defend the Global Information Grid (GIG). Each DoD Component then hires, trains, and retains the personnel that make all these things possible.

Finally, there is our secure information sharing partnership with mission partners, to include the Intelligence Community, industry, academia, international, federal, state, local, and tribal entities, as well as coalition nations and forces. These groups work together to achieve cross-organizational information sharing, while securing sensitive information and addressing threats and vulnerabilities to global infrastructure. As industry and the academic community introduce newer, more efficient methods and technologies, these partners will help the DoD CIO solve the challenges related to technology insertion and refresh, and learn about and incorporate industry best practices as appropriate.

Together these partnerships will enable us to achieve much more than the collective individual achievements of these organizations.

TECHNOLOGY LEADERSHIP

As a technology leader, the DoD CIO promotes IT innovation across the Department—facilitating the Department's adoption of new approaches, methods, services, and devices. The DoD CIO organization spearheads the innovative application of technology to address warfighter and decision maker requirements. In addition, the DoD CIO is responsible for communicating the value of new technologies to the broader organization. New technologies, appropriately applied, can improve operational effectiveness, efficiency, and security. However, these benefits may not be obvious, and sometimes require supporting empirical data. Overall, the DoD CIO seeks to insert new technologies wherever possible to enhance mission performance.

The Department's ability to attract the next generation workforce, and to leverage their talents, depends upon DoD's ability to develop and maintain a robust technology environment. That next generation presents the Department with a unique opportunity to make great leaps in its ability to share information more effectively. Having grown up in a "connected" environment that is extremely agile, they are tech savvy and have integrated mobile devices and social networking into their lives. The DoD CIO guides the deployment of such technologies to more effectively accomplish the DoD mission. For example, the DoD CIO is:

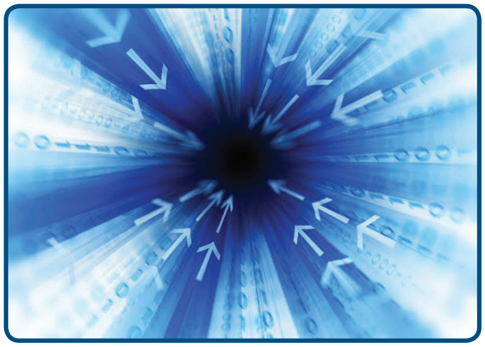
- Leading the effort to streamline the incorporation of mobile devices such as smart phones into our network environment, through actions like developing reciprocal certification and accreditation (C&A) practices and fielding DoD application (app) stores.
- Leveraging cloud implementations to enable effective, efficient, and secure storing, sharing, and manipulation of DoD data and PNT applications.
- Fostering the secure, responsible use of collaboration-enabling technologies across the Department to facilitate new, more agile, and innovative ways of getting the job done.

Finally, a foundational IT leadership challenge is managing the rapid fielding of new technologies. This challenge includes incremental development and fielding approaches and enabling the transition of successful pilots and technology demonstrations into fully implemented and supported initiatives or programs. Without inserting new technology concurrent with incremental development and fielding, programs will be delivered with yesterday's technology. Therefore, as a technology leader, the DoD CIO must pave the way for programs to deliver capability rapidly and for successful demonstrations to transition quickly to fully-sustained capabilities.

PURPOSE AND ALIGNMENT TO DOD MISSION PRIORITIES

The DoD CIO Campaign Plan presents our mission, vision, and strategic objectives, and serves as our roadmap to meet our objectives. Our mission is founded in the National Defense Strategy, the Quadrennial Defense Review (QDR), and the Defense Planning Guidance (DPG), as well as Presidential and Congressional guidance and direction. Development of the DoD CIO Campaign Plan was also informed by the DoD Strategy for Operating in Cyberspace and the Federal 25 Point Implementation Plan. The successful achievement of the strategic objectives and supporting actions will be critical to DoD's attainment of an information advantage and the achievement of Global Information Grid 2.0 (GIG 2.0) requirements. The DoD CIO Campaign Plan fully supports the Department's FY2012-FY2013 Strategic Management Plan's (SMP's) business goal for the DoD CIO, to "Build agile and secure information technology capabilities to enhance combat power and decision making while optimizing value." In particular, the Campaign Plan supports all four key SMP initiatives related to the business goal:

1. Execute the *DoD IT Enterprise Strategy and Roadmap* (ITESR).
2. Strengthen the oversight of Information Technology investments.
3. Integrate cybersecurity across the DoD Information Enterprise.
4. Develop long-term strategy to provide for and protect mission-critical access to radio frequency spectrum.



All the defined actions and tasks within the roadmap will be continually assessed and serve as the basis for future resource allocations.

CAMPAIGN PLAN ORGANIZATION AND EVOLUTION

Within this Plan, six Areas of Execution (AOEs)—all of equal importance—have been defined to support accomplishment of the goals of the 2010 – 2012 DoD Information Enterprise Strategic Plan. Each AOE section contains an overview of the AOE, the strategic objective that is addressed, and the priorities for accomplishment. The full Campaign Plan includes the supporting actions and tasks needed for success with expected completion dates and the office (or offices) of primary responsibility (OPR) within the DoD CIO staff. OPRs are accountable for the completion of their actions and tasks.

As the goals and the requirements of the Department evolve, the DoD CIO will adjust priorities and supporting actions as necessary. We will also take advantage of surging technological changes as well as applying process improvements and best practices learned from DoD partners in government and industry.

PART II

Part II presents a high-level view of the DoD CIO's six Areas of Execution. For each area, this summary provides the Strategic Objective, an overview of the priorities that focus actions and tasks within that area, and a description of the objective and relevance for each priority in that area.

The Areas of Execution are:

1. Provide Enterprise Policy and Architecture
2. Drive Secure It Infrastructure and Services
3. Forge Partnerships
4. Evolve the IT Workforce
5. Direct and Oversee DoD IT Investments
6. Strengthen Cybersecurity

PRIORITY 1.1: DEVELOP CIO POLICY FRAMEWORK

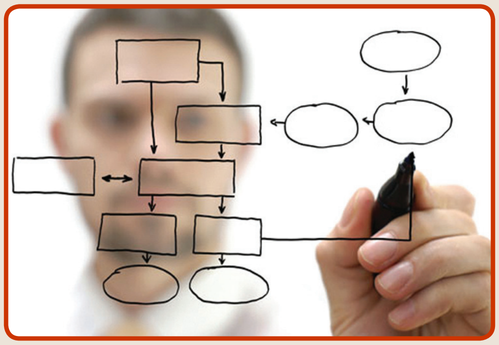
OBJECTIVE: Development of the policy framework to oversee and manage the integrated DoD IT architecture, and the information enterprise as a whole.

RELEVANCE: Aligned policies enable the rapid leveraging of emerging concepts and capabilities, and facilitate efficient and effective use of an integrated DoD IT architecture and the information enterprise as a whole.

PRIORITY 1.2: EVOLVE THE DOD ENTERPRISE ARCHITECTURE (EA) AND PROCESSES

OBJECTIVE: Consolidate and refine existing architecture and guidance into an overarching DoD Enterprise Architecture document that institutionalizes processes to support compliance with the DoD Enterprise Architecture.

RELEVANCE: Compliance with the DoD Enterprise Architecture ensures alignment of information capability initiatives under a common vision and enables the consistent use of standards for enhanced security and interoperability.



PRIORITY 1.3: STRENGTHEN CIO GOVERNANCE STRUCTURE

OBJECTIVE: Update the governance structure to guide and oversee the development and evolution of the DoD Information Enterprise to meet customer needs and strategic objectives.

RELEVANCE: A more effective governance structure provides a disciplined mechanism to attain Department-wide consensus and support for information enterprise solutions, including architectures, standards, and investments.

AOE 1: PROVIDE ENTERPRISE POLICY AND ARCHITECTURE

STRATEGIC OBJECTIVE

Provide enterprise policy and architecture to guide the development and delivery of secure, integrated information capabilities necessary for mission success.

OVERVIEW

Today, DoD forces increasingly rely on the DoD Information Enterprise for rapid access to information in support of mission success. Even in light of new operational and economic risks, the enterprise must strive to achieve improved levels of support for the warfighter. The DoD CIO will manage and evolve the DoD Information Enterprise to more quickly respond to threats, maximize capabilities with greater efficiency, and promptly embrace appropriate emerging technologies. To do this, the DoD CIO will establish an overarching management construct consisting of enterprise architecture, a policy framework, and governance. This management construct will guide the unified maintenance and evolution of the DoD Information Enterprise in alignment with customer needs and strategic objectives.

The DoD CIO will evolve the DoD Information Enterprise Architecture (DoD IEA) with associated standards, and the organizing framework for describing the DoD Information Enterprise. Together, these will guide the development of DoD information technology capabilities and enable the federation of DoD Component architectures to achieve a single, customer-focused vision of more consistent security, interoperability, and increased operational agility. Additionally, the DoD IEA will enable better analysis for more informed investment, design, and development decisions allowing leadership to logically manage the DoD Information Enterprise as a single cohesive unit.

In parallel, the DoD CIO will develop a policy framework—consistent with DoDD 8000.01, Management of the Department of Defense Information Enterprise—to ensure compliance with in-place authorities that enable the management and evolution of the DoD Information Enterprise. The policy framework will consolidate multiple processes for faster coordination, decision making, and resolution. It will promote an enterprise perspective to eliminate information stovepipes. Additionally, the DoD CIO will institute governance approaches to manage and evolve enterprise architecture and policy in alignment with operational requirements. The governance process will support consistent interpretation of policy, monitoring of DoD Information Enterprise performance, and timely addressing of customer issues.

PRIORITY 2.1: OPTIMIZE THE IT INFRASTRUCTURE BY PROVIDING COMMON SERVICES

OBJECTIVE: Consolidate IT infrastructure under common IT services to enable DoD to manage infrastructure as a commodity.

RELEVANCE: Use of common IT services increases efficiency by enabling the elimination of duplicative capabilities and making DoD's IT infrastructure more cost effective to maintain and more responsive to operational demand.

PRIORITY 2.2: INTEGRATE NETWORK TRANSPORT CAPABILITIES

OBJECTIVE: Ensure the integration, interoperability, and synchronization of information transport capabilities in the space, aerial, terrestrial, maritime, and cyberspace domains through participation in the Joint Capabilities Integration Development System (JCIDS); Planning, Programming, Budgeting, and Execution (PPBE); and Defense Acquisition System (DAS) processes.

RELEVANCE: More integrated systems and networks will provide improved interoperability, security, and overall operational effectiveness and efficiency.

PRIORITY 2.3: ENABLE SECURE INFORMATION SHARING AND INTEROPERABILITY

OBJECTIVE: Enable all authorized users to have immediate, secure, and reliable access to the information they need to perform their missions and support effective and agile decision making.

RELEVANCE: The establishment of the foundation for discovery, accessibility, understandability, and trust of data is essential to achieve enterprise-wide secure information sharing. The DoD CIO will lead efforts to implement and align the required strategies (e.g., Federal Information Sharing), policy, and guidance (e.g., DoDD 8320.02, DoDI 8320), standards (e.g., National Information Exchange Model (NIEM), data tagging), and implementation of data management initiatives such as Controlled Unclassified Information (CUI) and Records Management.

PRIORITY 2.4: DEPLOY ENTERPRISE SERVICES

OBJECTIVE: Implement a suite of DoD Enterprise Services (ES) accessible by authorized users anywhere, anytime, while stationary and mobile, from tactical edge to sustaining base.

RELEVANCE: Implementing a robust set of DoD Enterprise Services will enable the rapid deployment of warfighter focused capabilities as well as increased efficiencies by leveraging the Department's massive economy of scale.

PRIORITY 2.5: IMPLEMENT IDENTITY AND ACCESS (IDAM)

OBJECTIVE: Provide timely access to information using authentication infrastructure that provides Dynamic Access Control capabilities granting authorized users access to information assets based on established enterprise identity attributes that contain biographical, contextual, and biometrics data.

RELEVANCE: Access based on fraudulent identity is a recognized vulnerability for US National Security by asymmetric and cyber threats. The DoD CIO has a critical role in synchronizing identity issues across the Department for application in all mission environments. Department-wide IdAM capabilities will replace today's decentralized, manually-intensive, organizationally-unique, static access control mechanisms that are becoming increasingly inefficient and unresponsive to DoD access needs and complicate non-repudiation for insider threats.

PRIORITY 2.6: TRANSITION TO CLOUD COMPUTING ENVIRONMENT

OBJECTIVE: Drive delivery and adoption of a secure, dependable Enterprise Cloud Computing Environment to enhance mission effectiveness and improve IT efficiencies to meet mission needs and support anywhere, anytime, information access.

RELEVANCE: The transition to a cloud environment is a key enabler for the Department's Mobility Strategy and IT Consolidation efforts to deliver the next generation IT environment, from the continental United States (CONUS) to the tactical edge.

PRIORITY 2.7: MANAGE SPECTRUM

OBJECTIVE: Ensure DoD Spectrum access to meet warfighting needs.

RELEVANCE: Access to the electromagnetic spectrum enables warfighters to use many technologies, including, radar, navigation, weapons, and communications systems. Future technologies will utilize spectrum as the foundation for wireless capabilities, which are essential to extending net-centric capabilities to the "tactical edge". However, spectrum is a finite resource, and its use must be carefully managed.

PRIORITY 2.8: ENSURE NATIONAL LEADERSHIP COMMAND CAPABILITIES (NLCC) ASSURED CONNECTIVITY

OBJECTIVE: Provide a robust DoD process and vision for producing assured, reliable, and enduring national-level command, control, and communications capabilities utilizing a set of secure and non-secure national Leadership Command Information Services and information environment

RELEVANCE: Carries out the national guidance and DoD policy to develop a national and nuclear C2 capability; provide secure, integrated, continuity of government communications to the President, the Vice President, and at a minimum, Category I executive departments and agencies; and establish NLCC as the DoD construct for information integration, supporting national leadership planning, situational awareness, and decision making.

PRIORITY 2.9: IMPROVE JOINT C2 CAPABILITIES

OBJECTIVE: Provide strategic direction, policy guidance, and oversight to enable the Department to effectively define, prioritize, acquire, govern, manage, and implement C2 capabilities in support of DoD operations.

RELEVANCE: Establishes and implements the Department's overall C2 strategy, approach, structure, and policies to enable enterprise-wide migration towards a service oriented environment and open architectures. Promotes more effective information sharing and integration of C2 capabilities at the national, strategic, operational, and tactical levels through the more efficient use of resources, common architectures and standards, software reuse, and data exposure.

AOE 2: DRIVE SECURE IT INFRASTRUCTURE AND SERVICES

STRATEGIC OBJECTIVE

Drive IT infrastructure and services that support an agile force by providing secure access to the information needed to perform their missions—anywhere, anytime.

OVERVIEW

In the objective DoD Information Enterprise, the IT infrastructure and services will support an agile force structure where DoD military, civilian, and contractor personnel—deploying and redeploying around the world to defend the nation and respond to man-made and natural disasters—have anywhere, anytime access to the information needed to perform their missions. Decision makers will have access to persistent, continuously available collaborative and knowledge management capabilities for secure information sharing to exercise authority and direct mission execution. Additional information capabilities will be rapidly deployed as enterprise services leveraging cloud computing technologies and streamlined acquisition processes. To provide authorized users with timely access to those capabilities and information, advanced IdAM policy, processes, and technologies will enable users to avoid inefficient, manually intensive registration processes. IT infrastructure (including hardware, software, services, processes, and spectrum) will be optimized for mission performance and affordability through the DoD IT Consolidation Near-Term Implementation Plan and other DoD CIO-led initiatives. Special emphasis will be placed on developing architectural and acquisition support to increase the utility of mobile end-user devices in the DoD business and tactical domains. Operating system, application, and IT hardware testing procedures, including the certification and accreditation processes, will be revamped to remove impediments to rapid capability delivery while effectively managing risk.

The DoD CIO leads efforts—to include the essential non-material items such as governance, policies, guidance, frameworks, architectures, and standards—to guide achievement of the objective DoD Information Enterprise, with the dual objectives of improving effectiveness of operations while also operating more efficiently. The Military Services, Combatant Commands, and Defense Agencies are responsible for implementing the material capabilities required to achieve the objective DoD Information Enterprise. In addition, the DoD CIO will lead implementation and use of performance indicators to track and demonstrate incremental progress toward achieving that goal.

PRIORITY 3.1: FOSTER MORE EFFECTIVE PARTNERSHIPS AT THE FEDERAL, STATE, LOCAL, AND TRIBAL LEVELS

OBJECTIVE: Ensure that partnerships with key federal, state, local, and tribal government organizations provide more timely situational awareness for decision makers and enable trusted collaboration.

RELEVANCE: Establishes a priority for partnering with federal, state, local, and tribal government organizations to ensure interoperability and information sharing with the Department. It provides opportunities for the Department to leverage products and best practices from other organizations.

PRIORITY 3.2: ESTABLISH CLEAR ROLES AND RESPONSIBILITIES WITH DOD AND NON-DOD PARTNERS ON NATIONAL LEADERSHIP COMMAND CAPABILITIES (NLCC) SUPPORT

OBJECTIVE: Strengthen and clarify DoD CIO partnerships with COCOMs, Services, and Agencies (CC/S/A), and create governance structures with clear strategies, priorities, accountability, and metrics.

RELEVANCE: Provides clarity on roles, responsibilities, and processes for which DoD CIO has a leadership role in conjunction with a CC/S/A.

PRIORITY 3.3: CULTIVATE AND DEVELOP PARTNERSHIPS WITH THE JOINT STAFF AND CC/S/A THAT ENSURE WARFIGHTERS RECEIVE APPROPRIATE DOD CIO SUPPORT FOR CONTINGENCY OPERATION INFORMATION AND COMMUNICATIONS (ICT) ISSUES

OBJECTIVE: Strengthen existing relationships and establish new processes/procedures to ensure ICT issues for the Warfighter that require DoD CIO involvement are visible and receive priority action for resolution, through partnerships with COCOMs, Services, and Agencies, and create governance structures with clear strategies, priorities, accountability, and metrics.

RELEVANCE: Ensures that CC/S/A ICT issues receive appropriate engagement from the DoD CIO in support of stability operations, humanitarian assistance, disaster response, civil/military information sharing, and contingency ICT.

PRIORITY 3.4: MAINTAIN AND STRENGTHEN PARTNERSHIPS WITH NATO AND OTHER KEY ALLIES AND PARTNERS TO ENABLE INFORMATION SHARING AND SECURE COLLABORATION IN SUPPORT OF OUR MUTUAL DEFENSE INTERESTS.

OBJECTIVE: Strengthen existing international relationships and guide DoD CIO cooperation activities based on goals and policy specific to activity, functional area, or nation.

RELEVANCE: Ensures effective interoperability and information sharing between DoD and NATO and other key allies and partners.

PRIORITY 3.5: ENHANCE DOD CIO STRATEGY AND COMMUNICATIONS

OBJECTIVE: Improve alignment of DoD CIO organizational responsibilities with our mission partners.

RELEVANCE: These plans direct and synchronize the actions of the DoD CIO organization over the next 500 days to evolve the information enterprise and maintain unhindered operational support.

AOE 3: FORGE PARTNERSHIPS

STRATEGIC OBJECTIVE

Form collaborative partnerships with internal and external stakeholders to deliver responsive mission essential capabilities, protect DoD equities, and ensure interoperability and reliability—by aligning strategic plans, architecture, and standards; balancing capital investments; and integrating doctrine and operational procedures.

OVERVIEW

The DoD CIO leads and enables a diverse range of collaborative partnerships with internal and external stakeholders, including international partners. The DoD CIO chairs and participates in the work of a wide array of Defense, interagency, and international boards and forums, and engages in the joint requirements, acquisition, and budgeting processes. Through such work, the DoD CIO guides DoD's Information Enterprise toward delivering discoverable, accessible, and trusted information sources and application services through judicious balancing of capital investments.

Effective international partnerships are critical to our success as an organization and as a Department. In support of the National Security Strategy and the National Military Strategy, the DoD CIO seeks to enable the allied national security community to exchange information and collaborate seamlessly and securely to ensure our shared objectives are achieved. The DoD CIO will contribute to an information environment, based on architecture and standards, that allows trusted partners to work together across a range of challenges to protect our collective interests.

Specific activities in developing effective partnerships include strategic dialogue, personal engagement, coordination of policy and standards development and promulgation, facilitating work with other OSD elements, negotiating formal agreements in areas of mutual benefit, representing partner issues to OSD, sharing technical and operational insights when appropriate, and acting as mediator when partner strategies and/or initiatives are in conflict. Additionally, in support of the National Military Strategy affirmation that NATO remains our Nation's preeminent multilateral alliance, the DoD CIO serves as the Department's representative to the NATO C3 Board, and promotes U.S. interests at NATO through robust participation in related capability panels, capability teams, and working groups.

PRIORITY 4.1: MANAGE THE IT / CYBERSECURITY FUNCTIONAL COMMUNITY WORKFORCE

OBJECTIVE: Apply the functional community management (FCM) framework for effective strategic planning and workforce sustainment.

RELEVANCE: An agile, highly skilled IT / Cybersecurity workforce is critical for dynamically operating, defending, and advancing the DoD Information Enterprise.

PRIORITY 4.2: STRENGTHEN THE IT ACQUISITION WORKFORCE

OBJECTIVE: Establish, maintain, and manage the IT acquisition career field competency model; certification standards; career paths; and position category descriptions.

RELEVANCE: Enhance the Department's development, management, and use of information technology by building a strengthened corps of highly skilled, trained, and experienced IT acquisition and IT program management professionals.

PRIORITY 4.3: ENHANCE IT / CYBERSECURITY RECRUITING AND RETENTION, EDUCATION, TRAINING, AND PROFESSIONAL DEVELOPMENT

OBJECTIVE: Recruit and retain, educate, train, certify, and continually develop opportunities to support a highly-qualified IT / Cybersecurity workforce.

RELEVANCE: A diverse set of IT / Cybersecurity recruiting and retention, education and training, and certification programs are key to maintaining an agile, highly-skilled workforce capable of operating, defending, and advancing the DoD Information Enterprise. Additionally, access to a variety of professional development opportunities serves as an attractive incentive for recruiting and retaining quality personnel. For optimum utilization, DoD IT/Cybersecurity personnel must have access to a variety of programs, both internally and externally, that are distributed through multiple learning delivery options.

AOE 4: EVOLVE THE IT WORKFORCE

STRATEGIC OBJECTIVE

Develop and sustain a broader, balanced current workforce and "workforce of the future" with the competencies and proficiencies necessary to operate, defend, and advance the DoD IE.

OVERVIEW

A holistic management approach is required to acquire and sustain a pipeline of well-trained, highly qualified IT/Cybersecurity professionals to support and defend DoD's Information Enterprise. The total DoD IT/Cybersecurity workforce community is composed of over 196,500 personnel (109,700 active duty and reservists and 86,800 civilians) who are resident in both typical IT occupations, as well as cross-cutting functional areas. These numbers and workforce mix are evolving to meet the Department's current, continuously emerging, and expanding mission requirements.

As the OSD IT/Cybersecurity Functional Community Manager, the Office of the DoD CIO provides oversight in the management of IT/Cybersecurity professionals within the military and DoD civilian workforce. Partnerships are formed across government, as well as with industry and academia, to influence and represent the interests of the DoD IT/Cybersecurity Community. The FCM works in strategic partnership with key stakeholders throughout the IT/Cybersecurity Community as well as other communities (e.g., the Office of Personnel Management, the Office of Management and Budget, and the Federal CIO Council).

The FCM framework enables management of the DoD civilian IT/Cybersecurity workforce—recruiting and retention, training, education and professional development across the Department. Overseeing civilian IT/Cybersecurity workforce management and reporting and partnering with the Component Functional Community Managers to develop competencies, career paths and training, as well as conducting capability assessments to close skill gaps impacting mission readiness, supports this priority.

The DoD IT/Cybersecurity workforce is a critical enabler to every element of the Department's evolving mission and functions. DoD's ability to create and leverage information superiority to carry out its missions depends on a highly skilled technical workforce prepared to effectively use and apply current and emerging information technologies to deliver mission capabilities while protecting the data, information, and infrastructures.

In addition to managing the IT/Cyber security workforce, the Office of the DoD CIO, as the IT acquisition workforce functional leader, is the proponent for the IT functional community within the defense acquisition workforce. Within DoD and across the federal IT acquisition landscape, a series of change initiatives is underway to improve the acquisition of IT systems, driven internally by DoD's need to acquire information technology and cyber capabilities more effectively and efficiently. Initiatives to strengthen the IT acquisition workforce are structured with the following goals in mind:

- Create a robust, sustainable IT acquisition workforce
- Develop a competency taxonomy and career roadmap
- Sustain learning and growth throughout the professional life cycle.

It is critical that all areas of the human capital management spectrum are managed to sustain a pipeline of agile IT/Cybersecurity/acquisition professionals with the experience, aptitude and creativity to meet the technological, cybersecurity and acquisition challenges of the Department. To address the constantly changing technological skill requirements, key workforce management initiatives such as recruitment and retention, education and training, and continuous development are addressed in this Area of Execution to build a strong sustaining force.

PRIORITY 5.1: MANAGE THE IT BUDGET

OBJECTIVE: To improve IT investment planning, programming, and budget processes to better oversee IT investment execution by enhancing the framework and processes for decision making on future programs.

RELEVANCE: To enhance the IT investment planning, programming, budget, and execution process for making informed decisions that support national defense policies and military strategies in meeting mission needs.

PRIORITY 5.2: ENHANCE THE IT ACQUISITION PROCESS

OBJECTIVE: To enhance IT acquisition process to more effectively manage the Department's investments in technologies, programs, and product support.

RELEVANCE: Enhancing the IT investment acquisition process will enable the Department to make better informed decisions that support national defense policies and military strategies in meeting mission needs.

PRIORITY 5.3: ENHANCE IT PORTFOLIO MANAGEMENT TOOLS

OBJECTIVE: Leverage tools and processes to support the management of the DoD IT portfolio.

RELEVANCE: Facilitates the categorization of investments, spending, program and portfolio performance, and return on investment. Supports the IT investment submission requirements of the Congress and OMB.

AOE 5: DIRECT AND OVERSEE DOD IT INVESTMENTS

STRATEGIC OBJECTIVE

Optimize the Department's IT investments in infrastructure, business systems, weapons systems, communications, and platforms to ensure mission success and efficient use of resources.

OVERVIEW

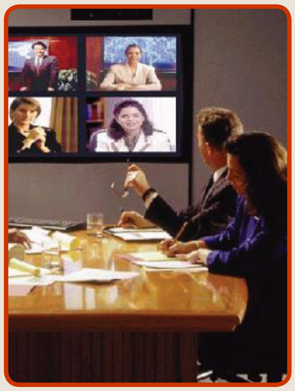
Making the best choices, identifying the right priorities, and managing resources to gain the most from investments is the charge from DoD senior leadership, the Congress, and the American taxpayer. It is also the central role of the DoD CIO in optimizing IT investments. The importance of that role is underscored by the $38.4 billion per year that the Department spends on IT investments including infrastructure, business systems, IT embedded in weapons systems, communications, and platforms.

Choices, priorities, and resources are managed through the direction and oversight conducted by the DoD CIO. That oversight includes those programs and capabilities that the DoD CIO is directly in charge of, as well as those capabilities led by partners and stakeholders. In each case it is critical to ensure that solutions across the Department of Defense can operate together, share information, and improve overall capabilities without causing unexpected problems or interference—in other words, be interoperable and function seamlessly. To have seamless operations, programs bringing new capabilities must follow established basic rules, principles, and standards. Consequently the DoD CIO is designated to ensure that programs are accountable and comply with the established rules, policies, and standards of DoD.

Optimizing IT investment and ensuring accountability and compliance with policy and guidance is made challenging by the distributive nature of program decisions that are spread across three major DoD processes: 1) the JCIDS, which supports the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying and assessing joint military capability needs; 2) the PPBE system, which produces a plan, a program, and, finally, a budget for the DoD; and 3) the DAS, which exists to manage the nation's investments in technologies, programs, and product support. Depending on the scope and importance, programmatic decisions are made at all levels of the DoD organization, such as by the military services and organizations within the services, employing these three major defense processes. DoD CIO IT investment oversight benefits the DoD through its involvement in these processes by looking across all major DoD IT investments and across multiple decision points. The DoD CIO meets its oversight responsibilities by appropriately engaging in the JCIDS, PPBE, and Acquisition processes and establishing DoD IT policies based on legislation and administration policy. To aid in these processes, the DoD CIO must furnish an effective toolset to provide decision makers with accurate and timely information.

Looking to the future, the Department realizes that it can improve the way it directs and oversees IT acquisition and manages information resources. The DoD CIO, in coordination with the Joint Staff, CAPE, the DCMO, and USD(AT&L), is looking across the Department for ways to reform IT acquisition. The new approach will be more streamlined, require fewer decision points and paperwork, reduce the "time to market," and drive more efficient IT resource management that supports federal green IT initiatives. The DoD CIO endorses and is helping to facilitate the reform efforts of how DoD invests in its IT capabilities while ensuring that it meets the true needs of the mission and the soldiers, sailors, airmen, and marines who execute it. In addition, the DoD CIO (in alignment with the Federal 25 Point Implementation Plan) will take a Cloud First approach to providing services whenever appropriate.

PRIORITY 6.1: ORGANIZE FOR UNITY OF PURPOSE AND SPEED OF ACTION



OBJECTIVE: Ensure the I&IA community establishes capabilities that work together as events demand, maintains an expected level of readiness, and that I&IA assets can rapidly be brought to bear. Ensure DoD I&IA capabilities work dynamically with those of our mission partners and DoD organizations understand the extended I&IA community, with each knowing its role.

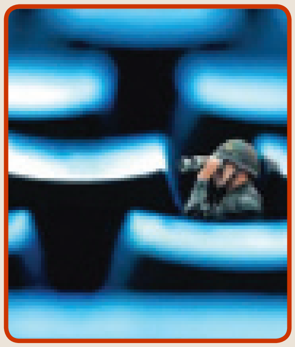
RELEVANCE: People and platforms can discover one another, can connect to form new capabilities, and can work together to achieve shared ends. Enables DoD to lead by setting enterprise direction, to deliver the right capabilities, and to leverage capabilities across organizations.

PRIORITY 6.2: ENABLE SECURE MISSION-DRIVEN ACCESS TO INFORMATION AND SERVICES

OBJECTIVE: Ensure DoD information is securely accessible to authorized users and every entity in the information enterprise has a unique digital identity; ensure adversary and neutral forces are identifiable; and provide strong identity authorization.

RELEVANCE: DoD information will not be disclosed to adversaries. Identity services will provide high confidence credentials for all entities (e.g., individuals, roles, devices). Improves ability to secure data in transit, manage access based on mission needs, and assure information sharing.

PRIORITY 6.3: ANTICIPATE AND PREVENT SUCCESSFUL ATTACKS ON DATA AND NETWORKS



OBJECTIVE: Identify and stop attackers outside or at the perimeter whenever possible, but also design and configure systems to ensure attackers are easy to find and contain should they pierce perimeter defenses. Better protect the GIG by aligning defenses across the enterprise.

RELEVANCE: The GIG will better withstand constant attack and better protect billions of dollars of DoD proprietary information being exfiltrated. DoD will align incident sources and will prevent attackers from getting in the GIG and from acting by constraining movement.

PRIORITY 6.4: PREPARE FOR AND OPERATE THROUGH CYBER DEGRADATION OR ATTACK

OBJECTIVE: Ensure cyber assets are trustworthy and that GIG operations have the means to prevail. Provide asset assurance that includes having confidence in suppliers, many of whom are globally sourced. Ensure operations can continue even with loss of all cyber capabilities.

RELEVANCE: The GIG will experience constant, highly sophisticated attack. DoD will foster trust in data and networks by guaranteeing integrity and availability of assets; will strengthen cyber-security readiness with coordinated event response; and will sustain mission-critical functions.

AOE 6: STRENGTHEN CYBERSECURITY

STRATEGIC OBJECTIVE

Build and operate DoD network capabilities as a joint global enterprise that more readily identifies and responds to cyber degradation or attack.

OVERVIEW

The United States, its friends, and allies face a world of complex challenges and great opportunities. Nowhere are those challenges and opportunities more apparent than in cyberspace. With information and IT assets distributed over a wide-ranging enterprise and with diverse domestic and international partners actively participating in DoD missions, the Department cannot execute operations without the GIG. The GIG is where intelligence data is fused; where weapons platforms are designed, built, and maintained; where commanders plan operations and command and control forces; where purchase and delivery of business goods and services are coordinated; where medical information resides; and where training, readiness, and morale and welfare are sustained. Maintaining freedom of action in cyberspace is critical to DoD and to the Nation. Therefore, the Department is focused on building and operating the GIG as a joint global enterprise. This enterprise network approach, coupled with skilled users, defenders, and first-responders, and in partnership with the intelligence and homeland security communities and the private sector, will allow the Department to more readily identify and respond to cyber degradation or attack—and still accomplish our missions.

The DoD Identity and Information Assurance (I&IA) strategy lays out four goals for creating effective capabilities, consistent implementation, and coordinated responses. Collectively, these goals describe an integrated approach for improving confidence levels and speed of action. They help organize and focus I&IA activities in the Department immediately and provide the long-term investment framework for realizing the Department's vision. These four goals are the priorities for this plan. To accomplish these four priorities, the DoD CIO will focus on these key areas in the near term:

- Establish policy, develop technology, and provide oversight to create and maintain strong, persistently monitored, and layered boundary defenses on DoD networks.
- Establish consistent privilege and configuration management processes for managing resilient GIG services, infrastructure, and information systems to achieve a secure, interoperable environment.
- Establish methods, policies, procedures, and desired capabilities with allies, as well as authorized mission, interagency, coalition, industry, and non-governmental partners to assure secure access to and protection of DoD, allied, and mission information.
- Promote development of international cyberspace norms and incorporate cyberspace into current international legal frameworks (e.g., Law of Armed Conflict) to increase the security and stability of DoD networks and the Internet.

REALIZING THE DOD CIO'S VISION

Realizing the DoD CIO's vision depends on a number of complementary efforts. The foundation is the DoD CIO's strong governance of the DoD Information Enterprise. The DoD CIO also works with the Components to align budgets to support IT efficiencies and to increase capability delivery. In addition, the DoD CIO is working with the Components to develop an integrated strategy that calls for a sequenced approach to the implementation of programs and initiatives through the IT Enterprise Strategy and Roadmap (ITESR).

These complementary efforts will produce a future DoD IT environment that is characterized by:

- Reduced Enterprise costs
- Improved interoperability
- Increased mission success
- Faster capability delivery
- Improved security
- Faster adoption of new technology

The DoD CIO is working across the Department to make this vision a reality. It will enable DoD and its partners to securely access information and services they need at the time, place and on the approved devices of their choosing.

LEVERAGING THE CAMPAIGN PLAN GOING FORWARD

This initial version of the plan provides a baseline for further analysis. DoD CIO leadership will build the next version of the Campaign Plan to include additional tasks necessary to achieve the DoD CIO vision and priorities. To accomplish this over the next few months, we will examine each AOE to identify gaps in the plan and capture tasks needed to fill identified gaps. DoD CIO leadership will then prioritize efforts, redirect resources, and descope, defer, or cancel less critical tasks as necessary to enable funding the efforts required to achieve our new priorities.

DoD CIO
6000 Defense Pentagon
Room 3E1030
Washington, DC 20301-6000