Department of Defense

Information Technology Environment

Way Forward to Tomorrow's Strategic Landscape.

Table of Contents

Introduction

Introduction

This is a time to be bold. DoD stands at a decision crossroad facing an information technology future that is fast moving, connected, and highly contested. Innovation continues to accelerate at a rate never-before seen, offering previously unimagined opportunities for the warfighter, coupled with a threat environment that also evolves at speeds previously unconceived. This is the new IT.

The Department's choice of cyber and IT toolsets lay the foundation for success – from the battlefield, to business, and beyond. Optimizing DoD's IT infrastructure by focusing on foundational IT changes that will advance capabilities, enhance the cybersecurity posture, and improve information sharing with mission partners is essential. In short, the Department's IT must have the same qualities expected from its Warfighters – innovation, collaboration, agility, adaptability, effectiveness, efficiency, and capability in defensive and offensive operations.

Today the number of organization-specific networks and computing systems used to execute missions, and the incremental manner in which IT is developed on a program-by-program basis, has resulted in a sub-optimal situation. The unnecessary complexity of the network and computing environment limits visibility and impedes the capability to securely share information and globally execute Joint operations. As the Department looks to the future, several key strategic areas of focus ensure DoD's IT will be able to meet the missions of today and support the strategic direction of tomorrow. Outlined in this document, they include:

- Executing capability initiatives toward the Joint Information Environment vision
- Improving collaboration with mission partners and industry
- Ensuring successful mission execution in the face of a persistent cyber threat
- Providing a cloud computing environment
- Optimizing DoD's data center infrastructure
- Exploiting the power of trusted information sharing
- Providing a resilient communications and network infrastructure
- Improving transparency, overnight, and execution of DoD IT investments

These changes require a new way of thinking – one that embraces the benefits that come with game-changing, yet proven, technologies and capabilities that will position the Department's IT infrastructure and processes for broader impact and greater security, in a mission- and cost-effective way. Agility, resilience, effectiveness – these have long-been the characteristics of Warfighters on the battlefront. As DoD faces a future where the battlespace has ventured into cyber and space, its IT infrastructure, investments, and capabilities should be held to the same standards.

Department of Defense Chief Information Officer

The DoD CIO is the principal advisor to the Secretary of Defense for (IT), cybersecurity; communications; positioning, navigation, and timing (PNT); spectrum management; senior leadership capabilities; nuclear command, control, and communications (NC3) matters, and the Joint Information Environment (JIE). These latter responsibilities are clearly unique to the Department, and the imperative of the DoD CIO is to ensure that DoD has the information and communications technology capabilities needed to support the broad set of Department missions. IT is critical to warfighting; command, control, and communications systems; computing services; cybersecurity; intelligence; and business missions.

The DoD CIO team includes the key cyber and IT leaders from all of the Military Services, United States Strategic Command (STRATCOM), United States Cyber Command (CYBERCOM), the National Security Agency (NSA), and the Defense Information Systems Agency (DISA). Together, these organizations are securing the Department's networks and systems, and managing the cyber threat from the infrastructure level down to each individual user. DISA serves as the operational arm for the Department's centralized IT environment, with DoD CIO oversight. DISA is a DoD combat support agency that provides IT and communications support to national leaders, the military services, the Combatant Commands, and more. It is comprised of more than 6,000 civilians and about 1,500 military officers and enlisted personnel, and approximately 7,500 defense contractors. DISA has a total budget of $9.4 billion out of a total DoD IT budget in fiscal year 2015 of approximately $36 billion.

Department of Defense IT Environment – Legacy Built and Complex

If the DoD was a corporation, it would be at the top of the Fortune 100 – no organization has a broader mission or scope. Comprised of 1.3 million military personnel on active duty, and 742,000 civilian personnel – plus 826,000 who serve in the National Guard and Reserve forces – DoD is one of the nation's largest employers. DoD also manages an inventory of installations and facilities, and its physical plant is vast by any standard, consisting of more than several hundred thousand individual buildings and structures located at more than 5,000 different locations or sites. When all sites are added together, the Department utilizes over 30 million acres of land. The Department also facilitates work streams in almost every business area. They vary from acquisitions, to command and control, to global logistics, to health and medical care, to intelligence, to facilities management – and each has an important role in cybersecurity.

The Department is similarly enormous on the enterprise network scale – by DoD numbers, it is the world's biggest enterprise network. As a snapshot, some of DoD's IT statistics include a DoD IT budget of more than $36 billion in fiscal year 2015, about ten-thousand operational systems, hundreds of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices. The Department's network must be mobile enough to support missions almost anywhere in the world, and flexible enough to facilitate collaboration with whatever partners a mission requires, expected or unexpected.

In this complex and wide-ranging IT environment, the number of organization-specific networks and computing systems used to execute DoD missions, and the systematic manner in which IT is developed through a highly regulated process, has resulted in a sub-optimal situation. The unnecessary complexity of this network and computing environment limits visibility and impedes the capability to securely share information and globally execute operations with mission partners. The current legacy environment offers too few enterprise and shared services. It is difficult to defend, and costly to operate and maintain. It also lacks the agility needed to fully support the dynamic mission environment. The complexity hinders the Department's ability to exploit the latest technology or share information internally or with allies as universally as required. Tomorrow's DoD IT environment will address this in close collaboration with industry through a seamless, transparent, resilient, secure DoD IT infrastructure that will empower simplified information sharing with mission partners.

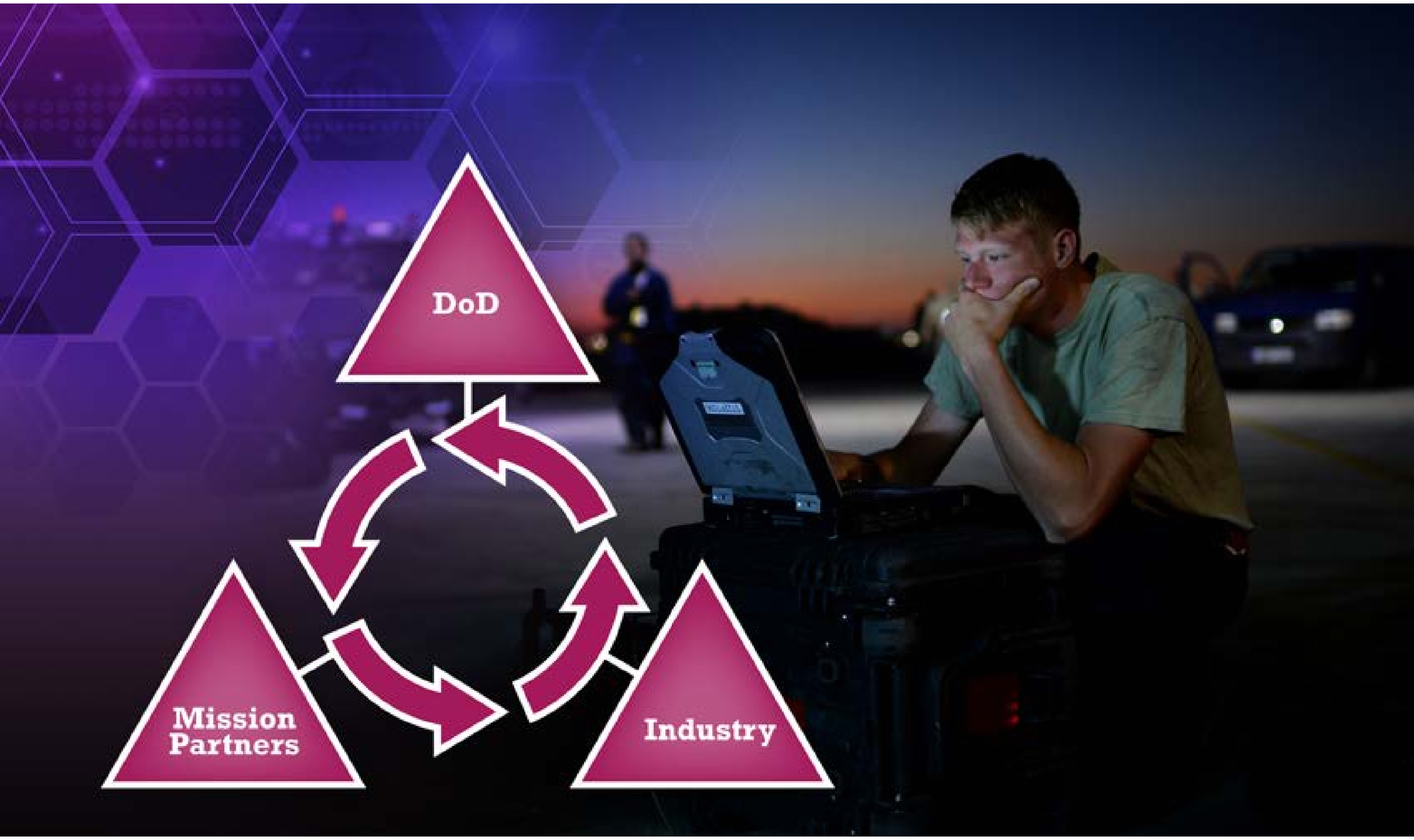
Vision for Tomorrow's DoD IT Environment

DoD IT of Tomorrow – Integrated, Resilient, Dynamic, Secure, Responsive

In today's strategic environment, warfare extends into space and cyberspace, and adversary capabilities in these areas can be expected to expand in tomorrow's strategic environment. A seamless, transparent infrastructure that transforms data into actionable information and ensures dependable mission execution in the face of the persistent cyber threat is vital in this new IT-driven operational environment. To accomplish this vision in an organization where IT spending is decentralized, more effective oversight of IT investments adds value. This will empower decision makers to understand where IT spending is going, and make the best decisions for the security, efficiency, and effectiveness of the DoD IT environment. DoD will not succeed without close collaboration with its industry partners, its mission partners, and other critical partners.

The "DoD IT Environment – Way Forward to Tomorrow's Strategic Landscape" is stet long-range path. DoD is considering a consolidated office automation and collaboration environment that delivers unified capabilities across DoD. This envisions a setting in which Commanders and warfighters can connect easily among themselves and with all of their critical mission partners in the same IT environment. DoD is working to ensure mission success in the face of cyber warfare by the most capable adversary. This envisions an environment in which any mission can be successfully executed in a threat-ridden cyber environment. DoD is ensuring that national assets in the DoD CIO portfolio – such as NC3, senior leader communications, and the Global Positionsing System (GPS) – are available, ready, and assured if or when needed. What happens to DoD, what happens to the U.S., what happens to the economy, if there is an incident, like a solar storm or a cyber-attack, that results in the failure of GPS? This envisions an environment in which that question is not answered. DoD is moving from a culture of compliance to a culture of risk assessment, transitioning to thinking about IT as a capability rather than as a program. How does DoD instill a culture that focuses on analyzing risk and fielding IT capabilities across the DoD workforce?

This document outlines this way forward to a more secure, effective, efficient DoD IT environment. This IT backbone and cyber defense posture are integral to tomorrow's DoD IT environment. Implementing capabilities for the JIE vision, including cloud computing, data center consolidation, and improving trusted information sharing, are vital. Improving transparency of the DoD IT budget improves centralized oversight of de-centralized DoD IT execution. Success in tomorrow's DoD IT environment will only happen standing next to its partners, so improving communication with mission partners and industry is vital. Finally, ensuring secure-enough, mission-appropriate cybersecurity will be a priority in this environment.



Way Forward to Tomorrow’s DoD IT

Goal 1: Execute Joint Information Environment (JIE) Capability Initiatives

Mission Impact: *A modernized IT enterprise with enhanced network performance that is more secure and visible throughout.*

Near-Term Focus: *The Joint Regional Security Stacks (JRSS) are a regionally based, centrally managed suite of network security appliances that will help simplify and secure the current DoD IT environment. JRSS is the near-term focus of the JIE capability initiatives.*

- ***Objective 1:*** *Implement JRSS and Associated Network Enhancements*
- ***Objective 2:*** *Shift from Component-Centric to Enterprise-Wide Operations and Defense Model*
- ***Objective 3:*** *Modernize Defense Information Systems Network (DISN) Transport Infrastructure*

Goal 2: Improve Partnerships with Allies and Industry

Mission Impact: *Positive synergies in processes, technologies, and intellectual capital are mutually beneficial to DoD and its partners. This will better support Joint/Coalition operations with mission partners, including the UK, Canada, Australia, and New Zealand (the Five Eyes); NATO, Germany, Japan, and others.*

Near-Term Focus: *The Information Technology Exchange Program (ITEP) will expand to twenty-five Government civilians serving in private-sector firms – as well as twenty-five Industry participants participating in DoD billets-by the end of fiscal year 2017.*

- ***Objective 1:*** *Partner Better with Industry*
- ***Objective 2:*** *Enable Information Sharing and Enhance Collaboration with Key Allies and Partners to Simplify Capabilities and Readiness*
- ***Objective 3:*** *Provide the Mission Partner Environment – Information System (MPE-IS)*
- ***Objective 4:*** *Streamline the Technology Approval Process*

Goal 3: Ensure Successful Mission Execution in the Face of the Cyber Threat

Mission Impact: *Provide mission dependability in the face of a capable cyber adversary.*

Near-Term Focus*: DoD CIO will revamp the Certification and Accreditation Process. Major DoD networks will migrate to Windows 10 by the second quarter of fiscal 2017.*

- ***Objective 1:*** Establish a Resilient Cyber Defense Posture

- ***Objective 2:*** Enhance Cyber Situational Awareness
- ***Objective 3:*** Assure Survivability Against Highly Sophisticated Cyber Attacks
- ***Objective 4:*** Evolve the Cybersecurity Workforce
- ***Objective 5:*** Ensure that Warfighting, Government Operations, and Intelligence Missions are Conducted in a Secure Communications Environment

Goal 4: Provide a DoD Cloud Computing Environment

Mission Impact: *DoD operations are supported with a new less complex, more agile and defensible IT environment that is more mission capable and less costly to operate. This increases mobility, virtualization, and integration of virtual services into DoD strategic environments.*

Near-Term Focus: Establish on-premise managed service capability by second quarter fiscal 2017.

- ***Objective 1:*** *Provide a Hybrid Cloud Environment*
- ***Objective 2:*** *Deploy Shared and DoD Enterprise IT Services via the DoD Cloud Environment*
- ***Objective 3:*** *Accelerate Delivery of New Applications and Digital Services*
- ***Objective 4:*** *Secure the DoD Cloud Environment*

Goal 5: Optimize the Department's Data Center Infrastructure

Mission Impact: *Optimized DoD computing infrastructure provides greater operational and technical resilience, improves interoperability and effectiveness, increases capability delivery, prioritizes secure capabilities, and reduces costs.*

Near-Term Focus: Establish a data center closure team to assess and recommend closures of the costliest and least efficient facilities beginning in the first quarter of fiscal year 2017.

- ***Objective 1:*** *Consolidate DoD Data Centers and Local Computing Infrastructure*
- ***Objective 2:*** *Rationalize DoD Applications and Systems for Migration into Core Data Centers (CDCs) and Component Enterprise Data Centers (CEDCs)*

Goal 6: Exploit the Power of Trusted Information Sharing

Mission Impact: *Enhanced support to decision-making processes — through secure access to DoD information and application of common data standards — improves collaboration both across the DoD enterprise and with external mission partners.*

***Near-Term Focus**: DoD is working on a two-year plan to eliminate Common Access Cards (CACs) from the Department's information systems. This effort includes working closely with NATO and Five Eyes partners on a consistent approach to credentialing.*

- ***Objective 1:** Deploy An Authentication Infrastructure To Dynamically Control Authorized User Access To Information*
- ***Objective 2:** Improve Information Sharing Across DoD and with External Mission Partners*
- ***Objective 3:** Integrate Commercial Mobile IT Capabilities*

Goal 7: Provide a Resilient Communications and Network Infrastructure

***Mission Impact:** Modernized DoD communications infrastructure and increased maneuverability within the electromagnetic spectrum provide greater operational and technical resilience, improved plug-and-play and effectiveness, faster capability delivery, prioritized secure capabilities, and reduced costs.*

***Near-Term Focus:** Continue modernization efforts to increase communications bandwidth in the DoD Information Network (DoDIN), like Nuclear Command, Control, and Communications (NC3) and Command, Control, Communications, Computers, and Intelligence (C4I) systems.*

- ***Objective 1:** Improve Strategic and Tactical Communications Networks*
- ***Objective 2:** Modernize Command, Control and Communications Systems*
- ***Objective 3:** Consolidate and Optimize Strategic Gateways*
- ***Objective 4:** Establish End-to-End Satellite Communications (SATCOM) Capabilities*
- ***Objective 5:** Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO)*
- ***Objective 6:** Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity*
- ***Objective 7:** Enhance the Delivery and Protection of (PNT)*

Goal 8: Improve Oversight and Execution of DoD IT Investments

***Mission Impact:** Strengthen DoD CIO's support to the Secretary in all matters regarding IT investments. Ensure that DoD IT investments are mission effective, cost efficient, and secure.*

***Near-Term Focus**: Optimize resources in a constrained fiscal environment to focus on DoD IT and cyber priorities, ensuring sufficient funding for cybersecurity and network security*

- ***Objective 1:** Review, Approve, and Align all DoD IT Investments with the Mission and Vision of the DoD CIO and Secretary of Defense*
- ***Objective 2:** Strengthen IT Financial Management Decision Making*

DoD CIO
6000 Defense Pentagon
Washington, DC 20301-6000
HTTP://DODCIO.DEFENSE.GOV/