DoD DIGITAL MODERNIZATION STRATEGY

DoD Information Resource Management Strategic Plan FY19-23

Change History

Version	Date	Page(s) Changed	Comments
1.0	5 June 2019		Signed version

Cancellation: This document supersedes the following:

- *Department of Defense Information Resources Management Strategic Plan*, April 1, 2014

Foreword

The global threat landscape is constantly evolving and remaining competitive and modernizing our digital environment for great power competition is imperative for the Department of Defense. We must act now to secure our future.

This Digital Modernization Strategy is the cornerstone for advancing our digital environment to afford the Joint Force a competitive advantage in the modern battlespace.

Our approach is simple. We will increase technological capabilities across the Department and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena. We will achieve this through four strategic initiatives: innovation for advantage, optimization, resilient cybersecurity, and cultivation of talent.

The Digital Modernization Strategy provides a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control and communications and cybersecurity.

This approach will enable increased lethality for the Joint warfighter, empower new partnerships that will drive mission success, and implement new reforms enacted to improve capabilities across the information enterprise.

The strategy also highlights two important elements that will create an enduring and outcome driven strategy. First, it articulates an enterprise view of the future where more common foundational technology is delivered across the DoD Components. Secondly, the strategy calls for a Management System that drives outcomes through a metric driven approach, tied to new DoD CIO authorities granted by Congress for both technology budgets and standards.

As we modernize our digital environment across the Department, we must recognize now more than ever the importance of collaboration with our industry and academic partners. I expect the senior leaders of our Department, the Services, and the Joint Warfighting community to take the intent and guidance in this strategy and drive implementation to achieve results in support of our mission to Defend the Nation.

David L. Norquist
Performing the Duties of the
Deputy Secretary of Defense

Executive Summary

The DoD Digital Modernization Strategy, which also serves as the Department's Information Resource Management (IRM) Strategic Plan, presents Information Technology (IT)-related modernization goals and objectives that provide essential support for the three lines of effort in the National Defense Strategy (NDS), and the supporting National Defense Business Operations Plan (NDBOP). It presents the DoD Chief Information Officer's (DoD CIO) vision for achieving the Department's goals and creating "a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat."[1] This vision is guided by four priorities and framed within four organizing goals.

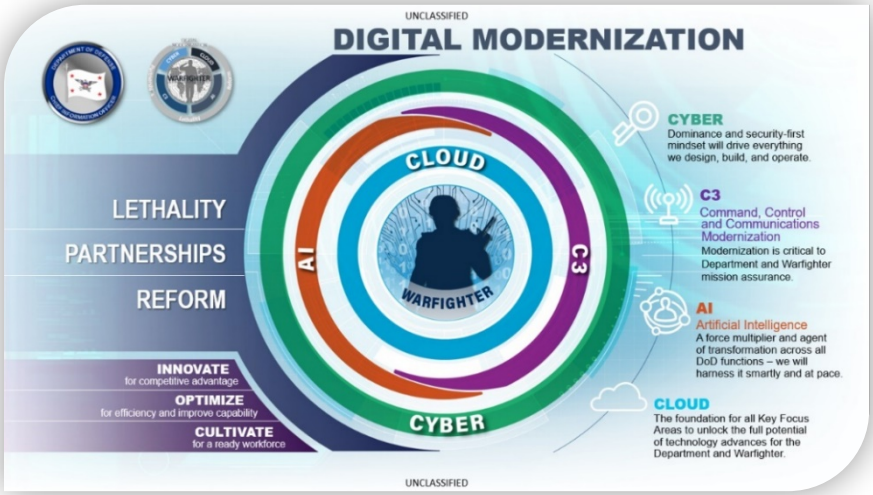


Figure 1: Digital Modernization

DoD CIO Priorities:

- Cybersecurity
- Artificial Intelligence (AI)
- Cloud
- Command, Control and Communications (C3)

Digital Modernization Goals:

- Innovate for Competitive Advantage
- Optimize for Efficiencies and Improved Capability
- Evolve Cybersecurity for an Agile and Resilient Defense Posture
- Cultivate Talent for a Ready Digital Workforce

[1] *DoD IT Environment – Way Forward to Tomorrow's Strategic Landscape*, August 2016 – available at http://dodcio.defense.gov/

This strategy also fulfills the Office of Management and Budget (OMB) requirement to provide a description of how information resources management activities help accomplish agency missions, and ensure that information resource management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.[2] It includes narratives that summarize the Department's approach to IT modernization, focused on the Joint Information Environment (JIE) Framework (in Section 3), and describe how Cybersecurity is being strengthened (Section 4). These efforts support achievement of the DoD CIO's modernization vision, and the goals and objectives identified in this strategy. Finally, appendices provide a brief description of promising technologies; tables showing alignment to the NDBOP, the President's Management Agenda, and DoD IT Reform Initiatives, respectively; and a summary of DoD CIO authorities.

[2] OMB Circular A-130, "Managing Information as a Strategic Resource" - available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

Contents

Context

If the Department were a corporation, it would be at the top of the Fortune 100. No organization has a broader mission or scope. DoD is also one of the nation's largest employers, with 1.3 million active duty military personnel, 742,000 civilian personnel, and 826,000 National Guard and Reserve forces. It manages an inventory of installations and facilities consisting of several hundred thousand individual buildings and structures at more than 5,000 different locations covering over 30 million acres of land. The Department also conducts major activities in almost every business area. These vary from acquisitions to command and control, global logistics, health and medical care, intelligence, space operations, facilities management and more—each with critical IT and cybersecurity dependencies.

The Department is similarly enormous on the enterprise network scale, operating one of the world's largest and most complex set of networks. As a snapshot, some of DoD's IT statistics include a budget of more than $46.4 billion in fiscal year 2019, roughly ten thousand operational systems, thousands 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 networks must be mobile enough to support missions around the world, and flexible enough to facilitate collaboration with any partners a mission requires, expected or unexpected.

This strategy highlights DoD CIO-led efforts that are key enablers for accomplishing the Department's missions more effectively and efficiently. The DoD CIO is responsible for all matters relating to the DoD Information Enterprise (IE)[3] Most efforts in this strategy therefore fall within the JIE Framework, which improves networking capabilities for fixed and mobile users, institutes new DoD-wide enterprise IT services, modernizes technology through coordinated refresh efforts, implements a new joint cybersecurity capability, and improves access to data. The JIE Framework also provides a networking design that improves defenses against malicious cyberspace activity and is managed through a tiered structure of network operations and security centers.

[3] As noted in Department of Defense Directive 5144.02, "The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2)." This directive is available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514402p.pdf

Role of the DoD CIO

The DoD CIO is the Principal Staff Assistant (PSA) and senior advisor to the Secretary of Defense for information technology (IT) (including national security systems), information resources management (IRM) and efficiencies. The DoD CIO is responsible for all matters relating to the DoD Information Enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD Information Enterprise that supports DoD command and control (C2). 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. The DoD CIO is a vital member of the Office of the Secretary of Defense (OSD) staff that helps the Warfighter by fulfilling its PSA and Clinger-Cohen Act (CCA) roles that guide the Department in the incorporation of more agile, efficient and effective technology and practices.

The DoD CIO works closely with other DoD and OSD Components in fulfillment of its responsibilities. As appropriate, the DoD CIO collaborates and coordinates with organizations including (but not limited to) the Chief Management Officer (CMO), the Office of the Under Secretary of Defense for Policy (OUSD(P)), the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), the Military Departments (MILDEPS), Joint Staff, and the Combatant Commands.

1 DoD Goals and Objectives

The DoD Digital Modernization Strategy, which also serves as the Department's Information Resource Management (IRM) Strategic Plan, aligns with and responds to high-level guidance for the Department, to include the President's National Security Strategy (NSS), the Department's National Defense Strategy (NDS), the Chairman of the Joint Chiefs of Staff's National Military Strategy (NMS), the National Defense Business Operations Plan (NDBOP), the DoD Cyber Strategy and the Defense Planning Guidance (DPG). The DoD Digital Modernization Strategy will also be supported through subordinate strategies for each of the four DoD CIO priorities, as shown in Figure 2, and other key topics where deemed appropriate.

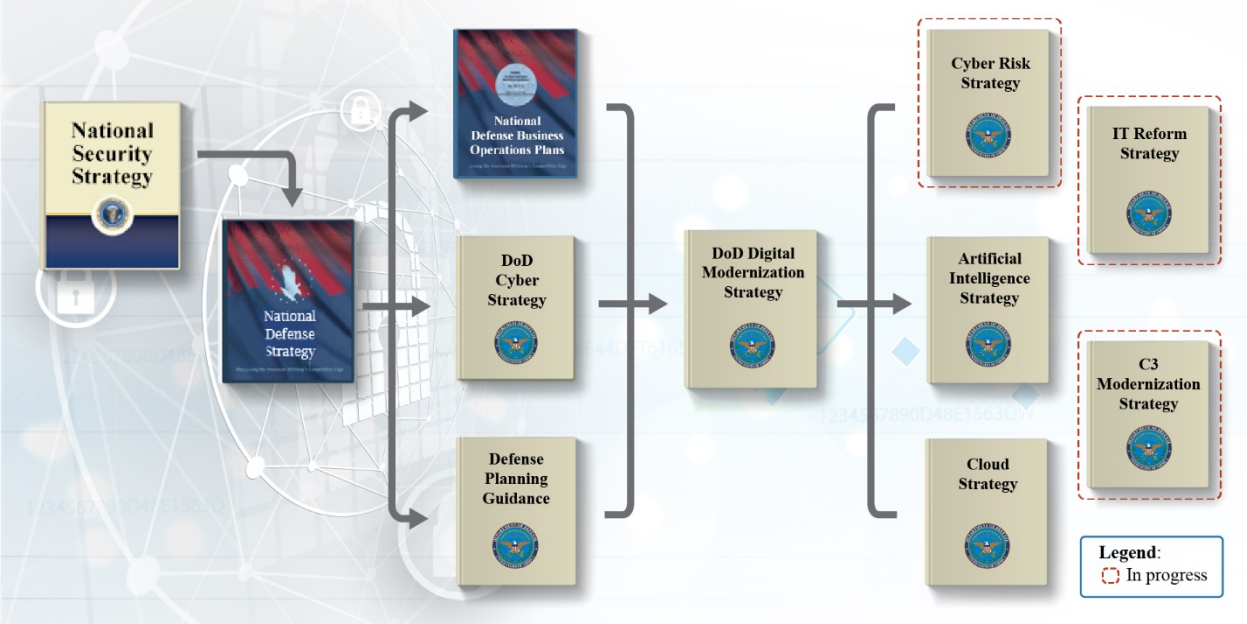


Figure 2: Alignment with National and DoD Guidance

The NDS establishes the Department's core strategic goals and guides planning for military force structure, force modernization, business operations, mission support infrastructure, and required resources. The DPG provides goals, priorities, and objectives, including fiscal constraints, for the development of each Military Department's Program Objective Memorandum (POM) and Budget Estimate Submissions (BES). The NDBOP is the OMB-mandated DoD Agency Strategic Plan (ASP) and the Department's roadmap for managing and reforming the business operations and mission support infrastructure needed to sustain the warfighter.

The NDBOP's strategic goals for Fiscal Years (FYs) 2018-2022 reflect the Department's priorities and strategic approach to the National Defense Strategy:

- Rebuilding Military Readiness as We Build a More Lethal Joint Force
- Strengthen Our Alliances & Attract New Partners
- Reform the Department's Business Practices for Greater Performance and Affordability

The NDBOP identifies building a more lethal force as the Department's principal goal, which aligns directly with the Department's mission to provide the military forces necessary to deter or

win war and to provide security for our nation. The NDBOP's strategic objectives contribute to increasing the capacity and lethality of military capabilities by ensuring that the warfighters have the best support available to prepare for their wartime missions. The NDBOP also identifies strengthening our alliances and attracting new partners as a key Departmental priority. It emphasizes that alliances and partnerships provide avenues for peace, foster conditions for economic growth with countries sharing the same vision, and temper the plans of those who would attack other nations or try to impose their will over the less powerful.

This strategy supports the NDS and NDBOP through the goals and objectives identified in Section 2. Each goal contains a set of objectives and supporting strategy elements. A strategy element defines a focused concentration of activities (initiatives) that are near-term and measurable. Many of the objectives and strategy elements are based on initiatives of the JIE Framework. Sections 3 and 4 provide related detail on the means to achieve the desired ends, while also addressing topics of interest to OMB, IT Modernization and Cybersecurity. The Appendices provide an overview of promising information technologies, a summary of DoD CIO authorities, and alignment with sources of strategic guidance and DoD IT Reform Initiatives.

2 Vision, Goals, Objectives, and Strategy Elements

Information Technology is a critical enabler for the command and control of forces executing warfighting operations, management and protection of information assets, and collaboration with mission partners. Initiatives in this strategy leverage innovative technologies, strengthen cybersecurity, cultivate talent, provide greater efficiency, transition the Department to DoD-wide and shared services, enhance our ability to collaborate with mission partners during conflict and response to natural disasters, and improve business practices. More effective, secure, and efficient IT will help preserve and expand our competitive military advantage and free additional resources for the Joint Force.

2.1 Vision of the Department's Future Digital Environment

The modern battlespace extends into space and cyberspace, and adversary capabilities in these areas can be expected to expand in tomorrow's strategic environment, increasing competition in and across all domains. To preserve and expand our military advantage in this new digital operating environment, the Joint Force must be adaptive, innovative and capable of seamlessly employing its capabilities across multiple regions and all domains. Agile, resilient, transparent, seamless and secure IT infrastructure and services that transform data into actionable information and ensure dependable mission execution in spite of the persistent cybersecurity threat are vital. Closer collaboration among DoD, its industry partners, and non-DoD mission partners will help DoD decision makers understand where IT spending should focus and enable better solutions in support of this vision.

However, more effective oversight of IT investments is necessary due to the decentralized nature of DoD operations and spending. Recognizing this need, Congress amended DoD CIO authorities and responsibilities, at Section 142 of Title 10, United States Code (U.S.C.), to include annual certification of Military Department and Defense Agency budgets, effective January 1, 2019. The DoD CIO will now oversee Department IT budget requests and modernization efforts with a comprehensive management system including both annual and multi-year processes as shown in Figure 3. The annual CIO Capability Planning Guidance (CPG) will provide programming and budgeting guidance in support of this system. That guidance will support this strategy and provide the primary basis for CIO Budget Certifications. This certification enhances established strategic planning, guidance, and scorecard processes.

Figure 3: DoD CIO Management System

This management system will enable continual, comprehensive Department-wide IT modernization in a common, coordinated way. Furthermore, it will accelerate transition to foundational enterprise capabilities and services, freeing DoD Components to focus on their mission-unique capabilities and services, as shown in Figure 4 below. Combined with policy and governance changes, it will shift the Department from an "opt-in" approach to enterprise services. Leveraging commonalities among DoD Component, the many overlapping and duplicative IT systems, programs, projects, services, capabilities, operations, and governance constructs in the Department will be more effectively synchronized, consolidated, and integrated.

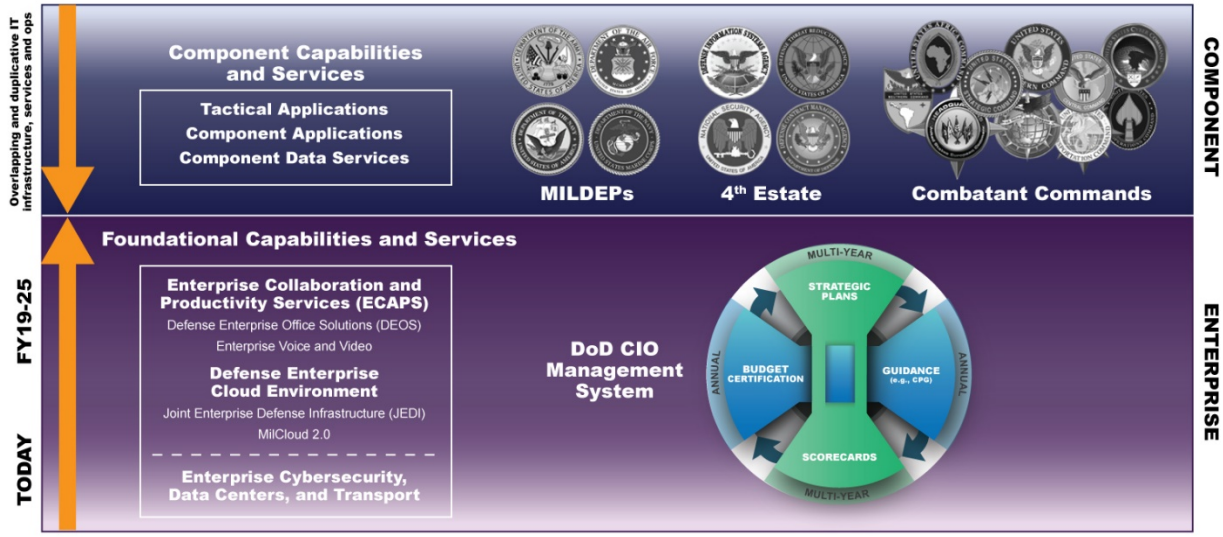


Figure 4: Shift to Foundational Enterprise Capabilities and Services

Benefits of this shift will include:

- Increased speed and reduced duplication of effort – increasing IT return on investment (ROI)
- Consistent, standardized enterprise IT architectures – supporting faster fielding of new capabilities, interoperability, usability, and improved cybersecurity risk exposure
- Increased budget transparency for DoD IT expenditures
- Convergence of Component network infrastructure – reducing complexity and cost
- Eliminates fielding of unnecessary capabilities and services – reducing program overhead
- Enterprise acquisition/licensing discounts – reducing infrastructure and application licenses

The future DoD digital environment will provide seamless, agile, resilient, transparent and secure infrastructure and services that advance DoD information superiority and simplify information sharing with mission partners. In accomplishing this, the future environment will leverage a number of innovative technologies, described in Section 3 and Appendix A, that promise to provide increased effectiveness, efficiency, and security.

2.2 Goals, Objectives, and Strategy Elements

This strategy outlines the way forward to a more secure, effective, and efficient DoD digital environment. Figure 5 below provides an overview of the goals and objectives.

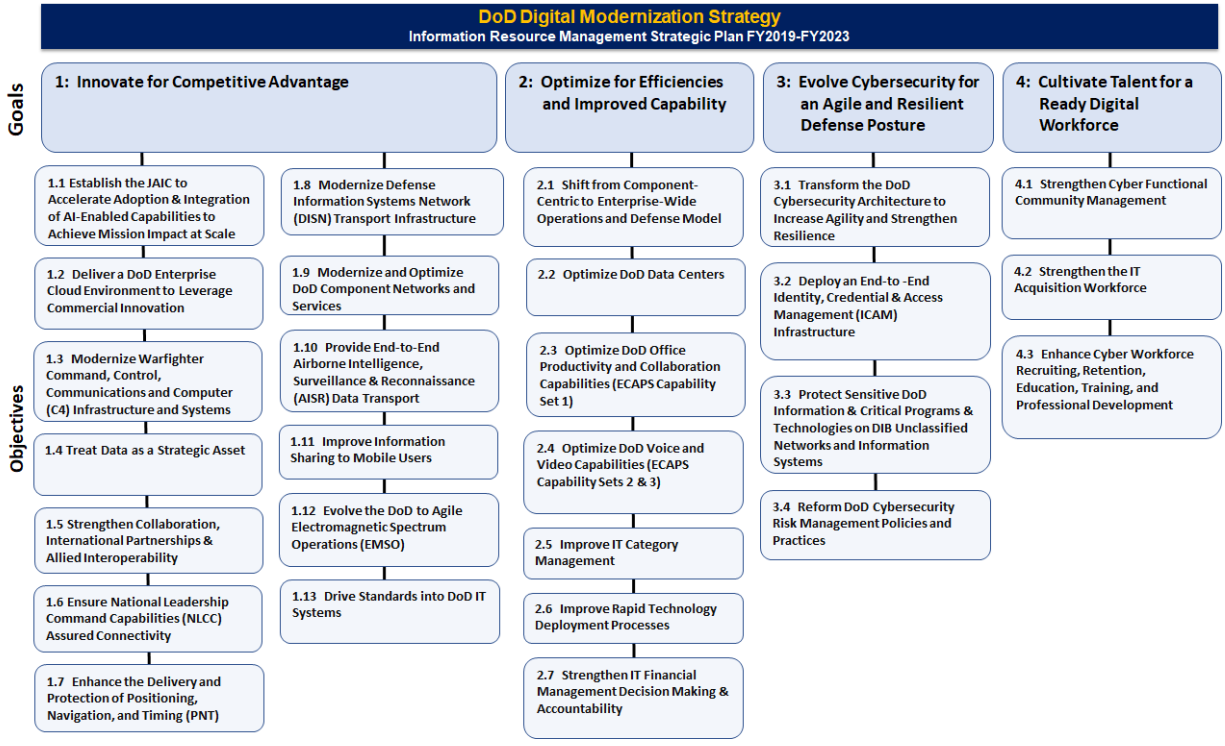


Figure 5: DoD Digital Modernization Strategy Goals and Objectives

Goal 1: Innovate for Competitive Advantage

Note: Each DoD CIO goal is presented with the following component parts:

- A **Description** of the goal, including what it encompasses
- The **Mission Impact** on the Department resulting from achievement of the objectives for that goal
- Each **Objective** has a **Description** that provides a rationale for the work and describes what the objective will accomplish
- Each objective is further decomposed into the **Strategy Elements** that describe the specific, focused initiatives needed to accomplish that particular objective

Description: Innovation is a key element of future readiness. It is essential to preserving and expanding US military competitive advantage in the face of near-peer competition and asymmetric threats. A theme running through the National Defense Strategy—and subordinate strategies like the Artificial Intelligence Strategy—is that preserving and expanding our military advantage depends on our ability to deliver technology faster than our adversaries and the agility of our enterprise to adapt our way of fighting to the potential advantages of innovative technology. The Department will evaluate opportunities for innovation, pursuing those deemed most suitable to address military problems and including those likely to deliver leap-ahead capabilities.

Cloud and cognitive computing will significantly alter warfighting and defense business operations. Recognizing this, the Department established the Joint Artificial Intelligence Center (JAIC) to accelerate delivery of AI-enabled capabilities and is partnering with industry to securely deliver commercial cloud capabilities in alignment with mission requirements. Modernization of warfighter support systems will enable improved command and control (C2), information sharing, and decision support, through a rich and diverse set of analytic capabilities fueled by data from sensors across the DoD Information Network (DODIN). Modernization of the Defense Information Systems Network (DISN), a key component of the DODIN, will provide critical enhancements necessary to fully realize the benefits from cloud computing, big data analytics, mobility, Internet of Things (IoT), increased automation and cognitive computing.[4] Increased availability and use of secure, mobile, wireless platforms across the Department will increase Joint Force maneuver, accuracy, and information advantage. Additionally, DoD will improve the efficiency and effectiveness of healthcare, logistics and other warfighting support functions. Enhanced delivery and protection of Positioning, Navigation and Timing (PNT), and development of a resilient, secure, and adaptive tactical IT infrastructure, will improve the Joint Force's ability to operate in denied, degraded, contested, congested, and operationally limited environments.

Central to many of these areas for innovation is software, which was highlighted in Sections 872-875 of the National Defense Authorization Act (NDAA) for FY2018 and the DoD 2018 Digital Engineering Strategy. Effectively managing the cost and speed of integration for software

[4] For information on the relationship between the DISN and the DODIN, please see Appendix B in the document entitled *Achieving the Joint Information Environment Vision*, released in August 2017. The JIE portal is the repository for this document (https://intelshare.intelink.gov/sites/dodjie).

delivery across the DoD is critical. Additionally, continued innovation in automating the software lifecycle beyond the current state of the practice will be required.

Mission Impact: This goal contributes to building a more lethal Joint Force (NDBOP Goal #1) by preserving and expanding competitive advantage. Additionally, it enables the strengthening of alliances and new partnerships (NDBOP Goal #2) by delivering dramatically improved collaboration capabilities. Transforming networks, system architectures, data management, electromagnetic spectrum operations, and enterprise service delivery also strengthen resilience, increase performance, and enable the Department to respond with greater speed and agility.

Objective 1: Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration of AI-Enabled Capabilities to Achieve Mission Impact at Scale

Objective Description: The commercial sector is in the midst of a revolution in AI that is reshaping business and society. The 2018 NDS highlights that AI "will change society and, ultimately, the character of war." The JAIC will accelerate DoD's adoption and integration of AI capabilities at speed and scale. It will operationalize AI capabilities by overcoming policy, technical, and financial roadblocks that prevent enterprise-level deployment, and by leveraging the capabilities established through DISN modernization (as described in Goal 1, Objective 8). The JAIC will collaborate with DoD Components (e.g. OUSD(R&E), OUSD(I), MILDEPS, Combatant Commands) to synchronize DoD-wide AI activities to enhance operational effectiveness and lethality, and increase efficiency of back-office business functions.

Strategy Elements:

- Strategy Element #1: Stand Up the JAIC and Initiate Operations
- Strategy Element #2: Establish Partnerships with Industry, Academia, and Partner Nations to Ensure State-of-the-Art AI Capabilities
- Strategy Element #3: Develop and Sustain the Enterprise Infrastructure Technology Stack that Enables AI Capability Deployment at Speed and Scale (JAIC Common Foundation)
- Strategy Element #4: Lead DoD in AI Planning, Policy, Oversight, Ethics, and Safety
- Strategy Element #5: Deliver AI-Enabled Capabilities to Address Key Missions (National Mission Initiatives, Component Mission Initiatives, and Smart Automation Initiatives)
- Strategy Element #6: Assure /Certify the AI Algorithms, Data, and Models Developed for JAIC Implementations

Objective 2: Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation

Objective Description: The advent of commercial cloud capabilities is changing the way DoD develops, delivers, deploys, and ultimately, buys applications, systems, and services. Cloud is the foundation upon which DoD will build and scale more effective cybersecurity, advanced analytical capabilities, better command and control, and future enabling technologies. This foundation will enable the Department to organize massive amounts of data and support rapid

access to information for improved decision-making, preserving and extending our military advantage. To better take advantage of this information, the optimized enterprise cloud environment will also provide a platform for advanced capabilities such as machine learning (ML) and AI that are necessary to increase decision-making quality, speed, and lethality. DoD will partner with industry to securely deliver commercial cloud capabilities in alignment with mission requirements and will manage these capabilities across the enterprise, to include the tactical edge (e.g., Denied, Degraded, Intermittent or Limited-bandwidth (D-DIL) environments), for improved effectiveness and efficiency. DoD CIO will collaborate with DoD Components (e.g., OUSD(R&E), MILDEPS, Combatant Commands) to support achievement of this objective.

Strategy Elements:

- Strategy Element #1: Deliver a General-Purpose Enterprise Cloud for Compute and Store Capabilities (i.e., Joint Enterprise Defense Infrastructure (JEDI))
- Strategy Element #2: Identify Common Niche Capabilities to Inform the Creation of Fit for Purpose (F2P) Cloud Environments
- Strategy Element #3: Provide a DoD On Premise Cloud Environment
- Strategy Element #4: Establish an Enterprise Cloud Office to Enable Rapid Acquisition, Deployment, and Migration to Cloud Capabilities
- Strategy Element #5: Manage the DoD Portfolio of Cloud Capabilities
- Strategy Element #6: Develop Policy and Guidance to Modernize Application Development (e.g., Lean-Agile Practices)
- Strategy Element #7: Develop and Deploy a DevSecOps Environment that Enables Application Development and Accreditation at Speed and Scale Integrated with Defensive Cyberspace Operations
- Strategy Element #8: Develop Policy and Guidance on the Effective Application of DevSecOps Principles
- Strategy Element #9: Enable Resilient Operation of DoD Functions on Commercial Cloud Infrastructure

Objective 3: Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems

Objective Description: Guide DoD investment to modernize Joint/Allied/Coalition C4 capabilities that support and enable the Joint warfighter. In collaboration with DoD Components (e.g., OUSD(R&E), MILDEPS, Combatant Commands), outline the way ahead for future development, implementation, fielding, and sustainment of strategic and tactical C2 and communications systems. Ensure that solutions are operationally effective in D-DIL circumstances.

Strategy Elements:

- Strategy Element #1: Produce C4 Strategies, Roadmaps, Plans, and Architectures
- Strategy Element #2: Update and Publish Required Tactical Communications Policies
- Strategy Element #3: Synchronize Enterprise C4 Capabilities through Effective Governance
- Strategy Element #4: Modernize Tactical Radios and DoD Tactical Waveform Capabilities
- Strategy Element #5: Develop and Maintain the Enterprise Architecture for DoD Public Safety Communications
- Strategy Element #6: Implement DoD Global Enterprise Mass Warning & Notification (EMWN) Capabilities
- Strategy Element #7: Modernize the Global Command and Control System - Joint (GCCS-J)
- Strategy Element #8: Modernize DoD Satellite Communications Management and Control
- Strategy Element #9: Execute the Satellite Communications (SATCOM) Modernization Activities Driven by the Protected Satellite Communications Services (PSCS) Analysis of Alternatives (AoA), the Wideband Communications Services (WCS) AoA, and the Impending Narrowband Satellite Communications AoA
- Strategy Element #10: Formalize and Implement the Enterprise SATCOM Management and Control Reference Architecture

Objective 4: Treat Data as a Strategic Asset

Objective Description: The full benefits of decision-making, information sharing, cloud migration, AI, and other DoD objectives stated in this strategy are dependent upon DoD's data being visible, accessible, understandable, trusted, and interoperable as prescribed by DoD Instruction (DoDI) 8320.07. Data owners and their communities of interest (e.g., financial, logistics, healthcare, human resources, cybersecurity, records management) are responsible for much of the necessary work. However, essential infrastructure (e.g., IT services registry, meta data registry, authoritative data source registry) and defined, standardized data tags or labels do not currently exist. Additionally, the Department has no enterprise search capability to enable discovery of critical DoD data across its network security domains.

DoD CIO is collaborating with the DoD CMO and Joint Staff on initiatives to support this objective. Joint Staff is driving development of data standards supporting interoperability. Separately, the FY2018 NDAA established a comprehensive and detailed set of Congressional expectations for the DoD CMO with respect to the treatment of data, summarized as follows: 1) Establish policy and governance for Common Enterprise Data related to business operations and management; 2) Conduct pilot programs to extract this data from relevant systems; 3) Analyze that data to generate insights that answer critical operational and business questions;

4) Evolve the pilots into a Data Management and Analytics Shared Service; and 5) Develop an Implementation Plan. The DoD CMO outlined its approach to Congress in December 2018.

Strategy Elements:

- Strategy Element #1: Define a Minimum Essential Set of Enterprise Data Tags that Enable the Tenets of DoDI 8320.07
- Strategy Element #2: Invest In and Maintain the Infrastructure Required to Make DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable

Objective 5: Strengthen Collaboration, International Partnerships, and Allied Interoperability

Objective Description: Coordinate efforts across the DoD, North Atlantic Treaty Organization (NATO), Allies, and other international partners to advance warfighting interoperability and coalition operations. Deepen C4 capability and information sharing. Maximize communications, export/sales, and other Security Cooperation activities with allied partner nations.

The Mission Partner Environment (MPE) enables the DoD to collaborate, share information, and conduct operations with mission partners. MPE connects DoD with the whole of U.S. government, Federal, State, local, and tribal government entities, allies, non-governmental organizations, treaty and private sector organizations, and territorial mission partners on a global scale, and supports the full range of military operations, including humanitarian assistance and disaster relief. All Combatant Commands (CCMD) require network interoperability with mission partners to optimize cooperation with a multi-national force. MPE will enable rapid formation of Communities of Interest (COIs) through all phases of military operations and for training and exercises. MPE will provide mission partners access to a set of core services and operational tools for modernized mission execution.

Strategy Elements:

- Strategy Element #1: Develop Military Satellite Communications (MILSATCOM) Services, Infrastructure, and Standards with International Partners
- Strategy Element #2: Improve Tactical Communications Waveform Export Processes and Develop a Standardized Method to Address CCMD Connection Requests between US and Allied/Coalition Systems
- Strategy Element #3: Advance Civil Emergency Communications Planning with DoD, NATO, Allies, and Other International Partners
- Strategy Element #4: Ensure End-to-End Identity, Credential, and Access Management (ICAM) Interoperability with Key Interagency and International Partners at Appropriate Assurance Levels for the Information Being Shared
- Strategy Element #5: Develop Flexible and Robust Secure Cryptographic Products for Seamless Secure Foreign Partner Interoperability
- Strategy Element #6: Streamline Release Processes and Decision-making to Advance U.S. Security Cooperation

- Strategy Element #7: Implement the MPE Requirements and Portfolio Management Processes
- Strategy Element #8: Rationalize Coalition C2 and Intelligence Information Sharing Capabilities
- Strategy Element #9: Deliver the DoD MPE Capability and Services

Objective 6: Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity

Objective Description: The NLCC will provide diverse, accurate, integrated, survivable, secure, and timely assured communication pathways that allow national leadership to execute national and military command responsibilities.

Strategy Elements:

- Strategy Element #1: Evaluate Current Conferencing Capability and If Required, Develop a Methodology that Improves Secure, Survivable Conferencing
- Strategy Element #2: Enhance Current Data Collection and Display Processes to Provide Senior Leadership-Quality Decision-Making Information
- Strategy Element #3: Develop a Process that Delivers a Classified, Secure, and Mobile Solution that Meets Senior Leadership Requirements
- Strategy Element #4: Enhance the Security of the Supply Chain for Continuity of Operations, Continuity of Government, and Senior Leader Command, Control, and Communications System (SLC3S) Communications Programs

Objective 7: Enhance the Delivery and Protection of Positioning, Navigation, and Timing (PNT)

Objective Description: Ensure positioning, navigation, and timing (PNT) availability and access. Precision strike, navigation, and network synchronization are dependent on the accuracy and dissemination of PNT signals predominantly provided at the present time by the Global Positioning System (GPS) and terrestrial atomic clocks. Improving the capability of the Joint Force (and Allies as appropriate) to operate in a GPS-denied or GPS-degraded environment requires a two-pronged effort: 1) decrease reliance on GPS-centric solutions by using Modular Open Systems Approaches (MOSA) to incorporate promising alternative/complementary PNT capabilities into Joint Force PNT devices; and 2) As improvements become operationally available, increase military GPS resilience by incorporating modernized GPS satellite, control, and user equipment capabilities. The strategy elements within this objective support all three Department strategic goals: Increase Lethality, Develop Alliances, and Reform Business Practices.

Strategy Elements:

- Strategy Element #1: Pursue DoD Implementation of a Modular Open Systems Approaches and Collaborative Modeling and Simulation (M&S) Approach for PNT Capabilities
- Strategy Element #2: Develop and Publish the DoD PNT Science and Technology (S&T) Roadmap in Coordination with the Under Secretary of Defense for Research and Engineering (USD(R&E))
- Strategy Element #3: Track and Assist in Modifying Plans for Military GPS User Equipment (MGUE) Development and Production
- Strategy Element #4: Field Modernized PNT Capabilities with the Air Force and Our International Allies
- Strategy Element #5: Develop Navigation Warfare (NAVWAR) Partnerships with Closely Allied Nations
- Strategy Element #6: Evaluate and Demonstrate Complementary PNT Capabilities to Support Domestic Critical Infrastructure in Cooperation with Civilian Agencies (Department of Transportation (DOT) and Department of Homeland Security (DHS))
- Strategy Element #7: Exercise the DoD PNT Enterprise Oversight Council, Executive Management Board, and Supporting Working Groups, To Ensure the DoD PNT Enterprise Provides a Military PNT Advantage to the Warfighter
- Strategy Element #8: Develop New (and Maintain Existing) DoD Issuances to Facilitate Policy Implementation and Ensure DoD Component Compliance for the DoD PNT Enterprise
- Strategy Element #9: Continue to Institutionalize the PNT Data Repository Data Collection Process

Objective 8: Modernize Defense Information Systems Network (DISN) Transport Infrastructure

Objective Description: The promised benefits from cloud computing, big data analytics, mobility, IoT, increased automation, and cognitive computing can only be fully realized with a suitable network. Modernization of the DISN is necessary to improve performance, capability, capacity, agility, and security, while reducing cost and complexity. Greatly enhanced bandwidth capacity and increased network resiliency support use of DoD-wide services and consolidation of critical IT systems, applications, and services from local installations to core data centers and the DoD enterprise cloud environment. Convergence on Everything over Internet Protocol (EoIP) and demand for information services, such as streaming video and real-time collaboration capabilities, are further driving transport infrastructure bandwidth capacity and Quality of Service requirements. Modernization initiatives underway will drastically reduce the number of network connections needed at any given Base/Post/Camp/Station (B/P/C/S) by consolidating to an all-IP infrastructure sharing a common network connection that can be virtualized for specific mission needs and cybersecurity protection. Significant efficiencies will be gained by migrating

to a standardized set of protocols and network connection types, requiring fewer hardware types to operate, maintain, and refresh. The Joint Regional Security Stack (JRSS) improves mid-point network security, reduces attack surface, and improves situational awareness. Furthermore, it provides failover, diversity, mitigation, and resilient cybersecurity capabilities as a means to assure timely delivery of critical information to warfighters around the globe.

Strategy Elements:

- Strategy Element #1: Upgrade Optical Transport
- Strategy Element #2: Enhance Mid-Point Security by Implementing JRSS and Joint Management System (JMS)
- Strategy Element #3: Build Out Multi-Protocol Label Switching (MPLS) Router Network with Quality of Service and Performance Monitoring
- Strategy Element #4: Implement Software Defined Networking (SDN)
- Strategy Element #5: Eliminate Asynchronous Transfer Mode (ATM) and Low Speed Time Division Multiplexed (TDM) Circuits
- Strategy Element #6: Implement Internet Protocol version 6 (IPv6)

Objective 9: Modernize and Optimize DoD Component Networks and Services

Objective Description: In order to achieve a modernized and effective force, the Department needs to consolidate and streamline capability delivery to support an evolving mission environment. The Department requires a secure, consistent, and cost efficient network to conduct operations and business functions. Modernization of the DoD IT infrastructure requires a focus on network and service optimization that converges DoD networks, Service Desks, and Network/Service Operation Centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives. Standardizing and modernizing the IT infrastructure and services eliminates unnecessary systems and allows the Department to focus finite resources across fewer areas, ultimately shrinking the Department's threat surface in cyberspace. Additionally, this convergence should yield reduced facility utilization. The initial phase of this effort includes Fourth Estate organizations, with the objective to reduce the number of networking environments, move to a single service provider, and size the number of Network Operations Centers/Security Operations Centers (NOCs/SOCs) for greatest efficiency and effectiveness.

Strategy Elements:

- Strategy Element #1: Consolidate and Optimize Fourth Estate Networks
- Strategy Element #2: Consolidate the Number of Fourth Estate Service Desks into a Single Service Support Environment
- Strategy Element #3: Consolidate and Optimize the Fourth Estate Network Operation Centers/Security Operations Centers (NOCs/SOCs)
- Strategy Element #4: Establish Best Practices for Component Use of Commercial Service Providers in Their Optimization and Modernization Efforts

Objective 10: Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport (DT)

Objective Description: Develop programmed capabilities and non-material processes to provide end-to-end AISR DT capabilities to globally dispersed strategic, operational, and tactical consumers (DoD and mission partners) at the time, place, quantity, and quality they require. AISR DT capabilities are defined as the signal transmission systems and processes required to move data from airborne platforms to required data consumers at the point of need. In support of Joint Requirements Oversight Council (JROC) tasking,[5] DoD has established an AISR DT executive steering function and a joint Integration Task Force to provide direction for development of AISR transport capabilities and processes throughout the systems development lifecycle.

Strategy Elements:

- Strategy Element #1: Establish Capabilities to Support Ingest, Accumulation, and Global Delivery of AISR Data from Multiple Platforms/Sources
- Strategy Element #2: Build Tactical Relays for Sensor Platform Connectivity to Local Users and the DISN
- Strategy Element #3: Provide Global Satellite Gateways for Direct Beyond Line of Sight (BLOS) Connectivity Between AISR Platforms and the DISN
- Strategy Element #4: Establish Network Operations to Support End-to-End Situational Awareness and Proactive Network Management
- Strategy Element #5: Provide Direction for Future Platform Transport Capabilities

Objective 11: Improve Information Sharing to Mobile Users

Objective Description: The ongoing evolution of computing technology to mobile devices offers unprecedented opportunities to advance the operational effectiveness of the DoD. Through faster access to information and computing power from any location, field units will be able to maneuver in unfamiliar environments with real-time mapping and data overlay capabilities; friendly forces will be identified with greater accuracy; engineers and technicians will have streamlined identification and ordering of mechanical parts; and military healthcare providers will be able to better diagnose injuries and remotely access lab results while away from hospital premises. Additionally, by enabling real-time access to important management and productivity tools (e.g., e-mail, collaboration), warfighter support functions will be able to more effectively manage the business of the DoD. The end result of enhanced enterprise mobility will be:

- Increased availability and use of secure, mobile, wireless platforms across the Department—including within D-DIL circumstances

[5] 18 Apr 2017 JROCM 034-17; also see 7 Apr 2017 JROCM 028-17. The Knowledge Management Decision Support (KMDS) portal is the repository for JROC documents.

- Access to multiple classification levels of plug and play using authorized government devices with minimal configuration

Strategy Elements:

- Strategy Element #1: Streamline the Purchasing of Mobile Devices and Services across the DoD Enterprise
- Strategy Element #2: Improve Mobile Policies, Processes, and Procedures to Ensure Efficient and Effective Portfolio Management
- Strategy Element #3: Expand Use of Derived Credentials for Mobile
- Strategy Element #4: Develop Applications of Tactical Mobility
- Strategy Element #5: Establish a Mobile Device Security Architecture and Risk Management Approach in Collaboration with Five Eyes (FVEY) Mission Partners
- Strategy Element #6: Establish DoD Way-Ahead, Policy, and Plans for Use of the National First Responder Network (FirstNet) in Support of DoD Public Safety Communications
- Strategy Element #7: DoD Will Be an Early Adopter of 5G and Develop Applications to Leverage 5G Advanced Capabilities

Objective 12: Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO)

Objective Description: Develop a resilient, secure, and adaptive tactical IT infrastructure capable of operating within a contested, congested, and operationally limited EMS environment for Joint EMSO sensing, planning, management, and execution in order to enable U.S. dominance in all warfighting domains. DoD CIO will collaborate with DoD Components (e.g., OUSD(R&E), MILDEPS, Combatant Commands) to support achievement of this objective.

Strategy Elements:

- Strategy Element #1: Establish an EMSO Multi-Tiered Architecture Capable of Sharing EMS Data Between All Services and Agencies at All Classification Levels
- Strategy Element #2: Establish a Resilient, Secure, and Adaptive EMSO IT Network Infrastructure

Objective 13: Drive Standards into DoD IT Systems

Objective Description: As required by Section 909 of the NDAA for FY2018, the DoD CIO will lead development, implementation, and enforcement of an IT, networking, and cybersecurity standards process for the Department. DoD CIO will collaborate with Department stakeholders, such as OUSD(A&S), OUSD(R&E), and Joint Staff, in assessment and revision of the current processes, governance, policy, and standards. As part of this process, guidance for leveraging North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs), as well as commercial and governmental standards, will be provided. A critical desired outcome of this overall effort is increased interoperability. The DoD CIO envisions opportunities for synergy

between compliance with standards and the Department's overall digital modernization efforts.

Strategy Elements:

- Strategy Element #1: Assess and Identify Gaps in Policy for IT, Networking, Data, and Cybersecurity Standards
- Strategy Element #2: Develop Strategy for Addressing Gaps in Processes, Governance, Policy, and Standards
- Strategy Element #3: Implement Revised Processes, Governance, Policy, and Standards
- Strategy Element #4: Monitor and Enforce Compliance with Revised Processes, Governance, Policy, and Standards

Goal 2: Optimize for Efficiencies and Improved Capability

Description: Delivering IT capabilities with greater efficiency and performance requires the Department to reform the way it operates. In particular, the evaluation and implementation of suitable industry best current practices and proven technologies must be greatly accelerated, and oversight of IT spending must be improved. The objectives in this goal include shifting to an enterprise-wide operations and defense model; right-sizing DoD data centers; optimizing office productivity and collaboration capabilities, optimizing voice and video capabilities; improving purchasing through enterprise agreements; strengthening partnerships with industry; and strengthening IT financial management and accountability.

Mission Impact: This goal supports reform of the Department's business practices (NDBOP Goal #3). It accomplishes this through such means as deploying shared and DoD-wide services; rationalizing DoD applications and systems for migration into core data centers, component enterprise data centers, and the DoD enterprise cloud environment; streamlining the technology approval process; and strengthening IT financial decision making.

Objective 1: Shift from Component-Centric to Enterprise-Wide Operations and Defense Model

Objective Description: Shifting from Component Centric to Enterprise Network Operations will provide the capabilities necessary to enable operations centers—responsible for executing DODIN Operations and Defensive Cyber Operations-Internal Defense Measures (DCO-IDM) activities—to more effectively and efficiently secure, operate, and defend the DODIN. The vision is to ensure that DoD military commanders, civilian leadership, warfighters, coalition partners, and other authorized non-DoD mission partners have access to information and data provided in a secure, reliable, and agile DoD-wide information environment to enable C2 of forces performing cyberspace operations. The JIE Management Network enables operations centers to securely manage the DODIN and its elements. A fully converged DODIN IT Service Management solution is envisioned to support change management, configuration management, asset management, knowledge management, and service level management.

Strategy Elements:

- Strategy Element #1: Enable Global and Regional Operations Centers
- Strategy Element #2: Establish and Implement the JIE Management Network for JRSS
- Strategy Element #3: Converge DODIN IT Service Management (ITSM) Solutions
- Strategy Element #4: Converge DODIN Operation Common Operation Picture (COP) Solutions

Objective 2: Optimize DoD Data Centers

Objective Description: In accordance with Federal guidance,[6] DoD is optimizing the Department's data center facility footprint and the management and operation of those facilities. Ultimately, DoD's Information Enterprise will consist of a streamlined number of data centers that effectively and efficiently meet DoD's broad range of missions—from recruiting to acquisition management to command and control. As part of the optimization process, Installation Processing Nodes must be re-designated as Closing, an Installation Service Node, a Special Purpose Processing Node, or a Component Enterprise Data Center. The re-designation will be driven by an assessment of the systems and applications (if any) which must remain. DoD will migrate applications and systems to select data centers; optimize select data centers for performance first, then cost; and consolidate data centers where practical.

Strategy Elements:

- Strategy Element #1: Migrate DoD Applications and Systems that Cannot be Hosted in Commercial Cloud Environments to Enterprise Data Centers
- Strategy Element #2: Optimize Select Data Centers for Performance First, Then Cost
- Strategy Element #3: Re-designate Installation Processing Nodes in Accordance with the Department's Current Data Center Optimization Approach
- Strategy Element #4: Manage the DoD Data Center Inventory for Mission Need

Objective 3: Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)

Objective Description: DoD's cloud strategy is a main component in the overall efforts to modernize the Department's information technology, with the objective of achieving a Department-wide enterprise cloud computing ecosystem. As an integral part of that strategy, the Defense Enterprise Office Solution (DEOS) will enable the Department to improve interoperability and enhance cybersecurity across DoD operational boundaries. DEOS will put collaboration and productivity capabilities in the hands of every DoD employee and warfighter to more effectively and efficiently accomplish their missions. DEOS will offer an interoperable solution for timely and seamless collaboration and information-sharing across operational

[6] Federal data center optimization policy is available at: https://datacenters.cio.gov/policy/

boundaries and including D-DIL environments. DEOS is the first capability set solution within the DoD Enterprise Collaboration and Productivity Services (ECAPS) portfolio.

Strategy Elements:

- Strategy Element #1: Designate DEOS as a DoD Enterprise Service with all DoD Components Required to Adopt
- Strategy Element #2: Monitor and Assess All Pilots for Implementation Pitfalls and Challenges, including D-DIL; Roll All Lessons Learned from Early Cloud Adopters into DEOS
- Strategy Element #3: Field DEOS (including in D-DIL Environments) and Complete Migration of All DoD Users

Objective 4: Optimize DoD Voice and Video Capabilities (ECAPS Capability Sets 2 & 3)

Objective Description: Modernizing existing voice and video capabilities is critical for the Department to achieve integrated and seamless DoD-wide communication in an effective and financially sound way. Existing DoD voice and video services are largely outdated. They include a mix of obsolete circuit-based switch systems and video technology reliant on non-IP transport that is being phased out by commercial carriers. Eliminating these systems and transitioning to an integrated IP environment across Components will allow DoD to: 1) Optimize voice and video service, and 2) Effectively manage operating costs as commercial carriers escalate sustainment costs for remaining non-IP service. The DoD will also close a significant operational gap in current 9-1-1 capabilities and enhance force protection with the implementation of the Next-Generation 9-1-1 (NG911) national standard. Once implemented, that standard will operate on IP-enabled emergency networks—allowing constituents on DoD installations to make a 9-1-1 "call" from any communication device in any mode (e.g., voice, text, or video)—and provide interoperability with civilian mission partners.

Strategy Elements:

- Strategy Element #1: Define and Deploy an Optimized Enterprise Voice and Video Solution across the Department (e.g., ECAPS Capability Sets 2 and 3)
- Strategy Element #2: Define and Deploy an Optimized DoD C2 Voice Solution
- Strategy Element #3: Eliminate DoD's Legacy Analog Phone Switch Infrastructure
- Strategy Element #4: Establish DoD Way-Ahead, Policy, and Plans for Employment of Next Generation 9-1-1 (NG911)

Objective 5: Improve IT Category Management

Objective Description: Category management is an approach the Federal Government is applying to eliminate redundancies, increase efficiency, and deliver savings from acquisition programs. DoD is aligning its IT Category Management with the Federal IT Category Management efforts by pursuing strategic sourcing (e.g., enterprise license agreements (ELA)) for the acquisition of commercial IT software, hardware, services, and telecommunications.

DoD's IT Category Management is designed to save time and money by leveraging commercial IT requirements across DoD Components to negotiate more favorable terms in purchasing agreements and maximize discounts through enterprise volume purchasing solutions.

The result of IT Category Management will be:

- Decreased procurement overhead costs by reducing the number of duplicative commercial IT purchasing vehicles
- Reduced procurement costs by consolidating orders for common commercial IT
- Lower unit costs for common commercial IT goods and services by maximizing discounts through enterprise purchasing solutions
- Reduced costs of procuring and maintaining underutilized IT assets by improving asset visibility to reduce excess inventories
- Improved IT contract and license terms and conditions by using a qualified IT acquisition workforce to align enterprise agreements with DoD requirements
- Utilization of enterprise acquisition vehicles that enable the DoD to leverage economies of scale
- Improved product support services by including terms for minimum service levels for applicable commercial support services in enterprise agreements

Strategy Elements:

- Strategy Element #1: Continue to Establish ELAs for IT Software, Hardware, Services, and Telecommunications
- Strategy Element #2: Expand ELAs to Address Other IT Categories (e.g., IT Security) Based on OMB Guidance
- Strategy Element #3: Establish DoD Category Management Policy
- Strategy Element #4: Implement DoD IT Asset Management

Objective 6: Improve Rapid Technology Deployment Processes

Objective Description: One persistent challenge for DoD has been that acquisition processes have kept the Department from being able to adopt new technology in a timely manner. DoD will bring new technology in house much faster through three approaches: streamlining the technology approval process, leveraging innovative technology development practices such as Digital Engineering, and leveraging approved processes such as Other Transactional Agreements (OTAs). All of these approaches will enable the Department to reap the benefits of greater efficiency and security.

Strategy Elements:

- Strategy Element #1: Streamline the Technology Approval Process
- Strategy Element #2: Leverage the Power and Agility of Other Transactional Agreements (OTAs)

Objective 7: Strengthen IT Financial Management Decision Making and Accountability

Objective Description: The Component Financial Improvement Plans (FIPs), when summarized collectively, compose the Department's Financial Improvement and Audit Readiness (FIAR) Plan. The DoD Components' FIPs are prepared and executed in accordance with FIAR Guidance issued by the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)). The FIAR Guidance provides the strategy and standard methodology, as well as the step-by-step approach for discovery and evaluation; documenting, testing, and strengthening controls; and achieving an audit ready systems environment.

Existing and future systems will need to satisfy joint general and application level control requirements identified in the FIAR Guidance and the Federal Information System Controls Audit Manual (FISCAM). In addition, Departmental investments made in Internal Use Software, purchased (Commercial Off the Shelf (COTS)) or internally developed, must be accounted for in a manner that addresses financial statement auditability requirements.

To strengthen IT financial management and oversight, the FY2018 NDAA requires the DoD CIO to review each military department's and each Defense Agency's proposed budget against the responsibilities outlined in Title 10 USC 142(b) paragraph (1) and submit to the Secretary of Defense a report containing the comments of the CIO with respect to all such proposed budgets, together with the certification of the CIO regarding whether each proposed budget is adequate.

Strategy Elements:

- Strategy Element #1: Support Audit Readiness for Financial and Mixed Systems that Impact Financial Reporting
- Strategy Element #2: Improve Accountability and Auditability for Internal Use Software Investments
- Strategy Element #3: Implement FY2018 NDAA Requirements Regarding Oversight and Certification of Component IT Budgets

Goal 3: Evolve Cybersecurity for an Agile and Resilient Defense Posture

Goal Description: The scope, pace, and sophistication of malicious cyberspace activity continues to rise globally. Growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent issue that must be addressed. DoD overmatch in conventional and strategic weaponry may be overcome through sophisticated attacks within cyberspace, supply chain exploitation across the acquisition and sustainment lifecycle, and intelligence operations targeting insiders with access. The Department must adopt a "Cyber First, Cyber Always"[7] mindset and be prepared to defend DoD systems in a contested cyberspace. Every network, system, application and enterprise service must be secure by design, with cybersecurity managed throughout the acquisition lifecycle. The Department will maintain

[7] This phrase was used by the DoD CIO in his speech at the Billington Cybersecurity Summit on 6 September 2018.

system confidentiality, integrity, and availability by defending against avenues of attack used by sophisticated adversaries.

Mission Impact: This goal secures the information technologies and data that enable the Joint Force to gain information advantage, strike at long distance, and exercise global command and control. It supports all three NDBOP goals (Increase Lethality, Strengthen Alliances, Reform Business Practices) and the cybersecurity-focused objectives of the DoD Cyber Strategy. It achieves efficiencies by reforming the DoD Risk Management Framework; delivers capabilities to preserve the US military competitive advantage and assure mission completion; and strengthens collaboration with interagency, international and industry partners.

Objective 1: Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience

Objective Description: The Department's approach to cybersecurity is documented in the DoD Cybersecurity Reference Architecture (CSRA), which guides and constrains how network boundaries, mobile and fixed end points, and data are protected. The DoD CSRA is developed in collaboration with DoD Component stakeholders (e.g., OUSD(R&E), DISA, NSA, MILDEPS, Combatant Commands). It reflects key cybersecurity principles: isolation, containment, redundancy, layers of defense, least privilege, situational awareness, and physical/logical segmentation of networks, services, and applications. The resulting protections contribute to a resilient defense posture and achievement of three cybersecurity objectives:

- The DODIN—to include the data on the network—is defended as a virtual single information environment through the use of common processes and capabilities.
- Cyberspace-defenses sense and respond to external and internal threats and take appropriate remediation. mitigation. and restoration actions.
- Command and control of forces that operate on the DODIN is supported by shared cybersecurity situational awareness of the network as a whole. IT security findings are shared and reused throughout the Department to the greatest extent practical.

Strategy Elements:

- Strategy Element #1: Improve Endpoint Security and Continuous Monitoring
- Strategy Element #2: Enhance Enterprise Perimeter Protection Capabilities
- Strategy Element #3: Establish Enterprise Comply-to-Connect Capability
- Strategy Element #4: Deploy Insider Threat Detection Capabilities
- Strategy Element #5: Strengthen Data Center Security
- Strategy Element #6: Standardize on Windows 10 Secure Host Baseline (SHB)
- Strategy Element #7: Implement Automated Patch Management
- Strategy Element #8: Enhance Cybersecurity Situational Awareness through Big Data Analytics
- Strategy Element #9: Modernize the Cryptographic Inventory and Supporting Infrastructure

- Strategy Element #10: Incorporate Cloud-Native Capabilities into Defensive Cyberspace Operations

Objective 2: Deploy an End-to-End Identity, Credential, and Access Management (ICAM) Infrastructure

Objective Description: DoD must promote implementation of enterprise ICAM to support rapid access to mission information, strengthen responsible information sharing and attribution with allies and partners, and support greater effectiveness and efficiency through mobile adoption and migration to the cloud. ICAM encompasses the full range of activities related to creation of digital identities and maintenance of associated attributes, credential issuance for person/non-person entities, authentication using the credentials, and making access management control decisions based on authenticated identities and associated attributes. ICAM creates a secure and trusted environment where any user can access all authorized resources (including applications and data) to have a successful mission, while also letting DoD know who is on the network at any given time. Among its benefits, ICAM also supports correction of weaknesses reported in the notification of findings and recommendations (NFR) from the 2018 defense-wide financial audit.

Strategy Elements:

- Strategy Element #1: Expand Public Key Enablement Capabilities to Support ICAM
- Strategy Element #2: Implement Automated Account Provisioning
- Strategy Element #3: Implement Support for Approved Multi-Factor Authentication Capabilities
- Strategy Element #4: Enhance Enterprise Identity Attribute Service (EIAS)
- Strategy Element #5: Expand the Use of Derived Credentials
- Strategy Element #6: Implement a Data Centric Approach to Collect, Verify, Maintain, and Share Identity and Other Attributes
- Strategy Element #7: Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation
- Strategy Element #8: Deploy Shared Services Promoting the Implementation of Enterprise ICAM
- Strategy Element #9: Enable Consistent Monitoring and Logging to Support Identity Analytics for Detecting Insider Threats and External Attacks
- Strategy Element #10: Enhance the Governance Structure Promoting the Development and Adoption of Enterprise ICAM Solutions
- Strategy Element #11: Create DoD Policies and Standards Clearly Defining Requirements for Identification, Credentialing, Authentication, and Authorization Lifecycle Management

Objective 3: Protect Sensitive DoD Information and Critical Programs and Technologies on Defense Industrial Base (DIB) Unclassified Networks and Information Systems

Objective Description: DoD relies on the Defense Industrial Base to develop advanced technologies and warfighting capabilities. Adversaries exploit DIB unclassified internal networks and information systems, stealing sensitive information in order to kill, counter, or clone DoD's warfighting capabilities before they are delivered to DoD. To improve the safeguarding of this information, DoD CIO, OUSD(A&S), OUSD(R&E), the Principal Cyber Advisor, and other stakeholders are collaborating on a multipronged approach that incorporates voluntary cyberspace threat information sharing, mandatory cybersecurity standards for defense contractor unclassified internal information systems and networks, and cybersecurity reporting of incidents that affect DoD controlled unclassified information on defense contractor unclassified internal information systems and networks.

DoD CIO is a key stakeholder in the implementation of the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" requiring industry to implement adequate security for their information systems that process DoD controlled unclassified information, including at a minimum the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

DoD CIO also oversees the DIB Cybersecurity (CS) Program. The DIB CS Program is DoD's public-private cybersecurity threat collaboration partnership through which classified and unclassified cybersecurity threat information is shared with DIB participants. The DoD Cyber Crime Center (DC3) is the operational focal point for the program, analyzing cybersecurity threats, developing a common operational threat picture, and sharing mitigations with industry, DoD, and interagency partners. DC3 is also the designated single DoD focal point for receiving all cybersecurity incident reporting affecting unclassified networks of DoD contractors from industry and other government agencies.

OUSD(A&S) is utilizing pathfinders to assure DIB cybersecurity requirements and expand cybersecurity threat information sharing to non-cleared defense contractors. These pathfinders will examine (1) a standard cybersecurity maturity model certification for DIB companies, (2) external cybersecurity validation of DIB companies with on-premise Controlled Unclassified Information (CUI) data through commercial 3rd party companies, and (3) internal cybersecurity validation of DIB company volunteers with off-premise CUI data in commercial clouds through FFRDC and UARC partners.

Strategy Elements:

- Strategy Element #1: Support Development of Consistent Procedures to Assess Contractor Compliance with Cybersecurity Requirements
- Strategy Element #2: Support Efforts to Update NIST SP 800-171 to Address Advanced Persistent Threats
- Strategy Element #3: Increase Participation in the DIB Cybersecurity Program
- Strategy Element #4: Expand Cybersecurity Threat Information Sharing to Non-Cleared Defense Contractors
- Strategy Element #5: Plan and Execute DIB Cybersecurity Pathfinders

Objective 4: Reform DoD Cybersecurity Risk Management Policies and Practices

Objective Description: DoD will reform its cybersecurity risk management policies and practices to be more effective, yet responsive to the needs of the warfighter. DoD's risk management approach requires prioritizing critical systems and assets; identifying and mapping mission risks; and tailoring cybersecurity implementation to mission dependencies. Furthermore, increasing dependence on commercial technologies and services (e.g. commodity IT, Industrial Control Systems, cloud services), coupled with the interdependent nature of cyberspace, requires more robust engagement to increase international cooperation, pro-actively shape standards, expand the use of software and hardware assurance methods, and address global supply chain risks. Finally, the DoD Risk Management Framework process will be reformed to improve effectiveness and efficiency, while ensuring it does not unnecessarily hinder the development and deployment of systems supporting the warfighter.

Strategy Elements:

- Strategy Element #1: Advance Risk Management Framework Reform to Ensure it is More Efficient and Adaptable
- Strategy Element #2: Ensure Cybersecurity Risks are Planned for and Managed Throughout the Acquisition Lifecycle
- Strategy Element #3: Enhance Processes to Address Enterprise-Wide Supply Chain Risks
- Strategy Element #4: Strengthen the DoD Cybersecurity Portfolio Management Process
- Strategy Element #5: Expand the Use of Proven Software and Hardware Assurance Methods
- Strategy Element #6: Build and Maintain Robust International Cybersecurity Cooperation Efforts
- Strategy Element #7: Increase DoD Participation in Setting Federal Government and International Commercial Cybersecurity Standards

Goal 4: Cultivate Talent for a Ready Digital Workforce

Goal Description: Competition for high quality, experienced digital workforce personnel is constant and increasingly aggressive. The Department of Defense is one of the three largest markets for this talent in the United States due to its size, its continuous adoption and adaptation of technology, and its extensive mission requirements. Critical national infrastructure protection in particular is a global growth industry.

DoD is executing a new Functional Community Maturity Model for management of DoD civilians. The DoD CIO will implement this model for elements of the Cyber Workforce and expand implementation of more agile recruiting, training, and retention capabilities through expansion of the Cyber Excepted Service personnel system, incentives, and local supplements. Work continues on development of baseline qualification requirements for over 50 cyber work roles. This will provide the workforce with a common understanding of the concepts, principles, and applications of cyberspace functions to enhance interoperability across organizational lines and mission sets.

Mission Impact: Accomplishing this goal will produce an appropriately sized workforce of well-trained, highly qualified professionals to support and defend the DoD Information Enterprise. It will also develop an agile and responsive workforce management system capable of meeting the Department's current and emerging cyberspace mission requirements. This goal primarily supports rebuilding military readiness and increasing the lethality of the Joint Force (NDBOP Strategic Goal #1).

Objective 1: Strengthen Cyber Functional Community Management

Objective Description: Improve business practices to promote strategic management and development of the civilian cyber workforce.

Strategy Elements:

- Strategy Element #1: Implement the Functional Community Maturity Model for the IT and Cybersecurity Categories of the Cyber Workforce
- Strategy Element #2: Identify and Target Work Role Gaps of Critical Need for the Cyber (IT and Cybersecurity) Workforce

Objective 2: Strengthen the IT Acquisition Workforce

Objective Description: Develop and sustain a cyber workforce cadre skilled in the application of strategic planning processes and agile acquisition capabilities for the attainment of secure technologies and software.

Strategy Elements:

- Strategy Element #1: Strengthen IT Acquisition Workforce Competencies
- Strategy Element #2: Update Curriculum Requirements and Maintain Continuous Learning Capabilities

Objective 3: Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development

Objective Description: In 2018, DoD commenced conversion to a new, more agile personnel program developed specifically for the Cyber Workforce. This program will continue to expand in functionality and scope as additional organizations and individuals convert to Cyber Excepted Service, providing hiring managers with greater options for sourcing candidates and the ability to offer more competitive compensation packages. A new Cyber Workforce Qualification Program is also under development which incorporates flexible attainment of credentials and performance-based assessments to achieve a DoD-wide standard baseline of cyberspace capabilities.

Strategy Elements:

- Strategy Element #1: Expand Implementation of Cyber Excepted Service
- Strategy Element #2: Implement Cyber Workforce Qualifications Program

3 DoD IT Modernization

The Joint Information Environment (JIE) is a framework comprising a set of discrete initiatives developed and delivered as funded to support continual, comprehensive Department-wide IT Modernization and advance DoD information superiority in a common, coordinated way. JIE implements a new joint cybersecurity capability, improves networking capabilities for fixed and mobile users, institutes several new DoD-wide IT services, modernizes technology through coordinated refresh efforts, meets mission partner information sharing requirements, and improves access to data. JIE also provides a networking design that improves defenses against cyberspace attacks and network intrusions and is managed through a tiered structure of network operations and security centers. JIE is intended to improve mission effectiveness, increase cybersecurity, improve interoperability, deliver capabilities faster, and realize IT efficiencies.

The scope of the JIE effort consists of ten Capability Objectives comprising the JIE Framework. Each Capability Objective includes one or more major initiatives that help define essential aspects to be accomplished to achieve the vision. The JIE Framework is being managed through an agile, unifying approach to improving the Department's IT and cybersecurity capabilities.

The JIE Framework includes the primary networks (Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET)), coalition networks handling materials up to Secret and Secret/Releasable (S/REL), and deployed warfighter's communications connectivity to the sustaining base IT infrastructure. Figure 6 puts the scope of priority JIE infrastructure efforts into perspective. It includes key components, such as the Internet Access Points (IAP), JRSS, DoD data centers, satellite gateways (SATGW), Mobility Gateways (MGW), Multi-protocol Label Switching (MPLS)-enabled DISN optical transport network sites, and the Mission Partner Environment. JIE capabilities are intended to enable DODIN Operations and DCO-IDM at the global (enterprise-wide), regional, and DoD Component/mission levels.

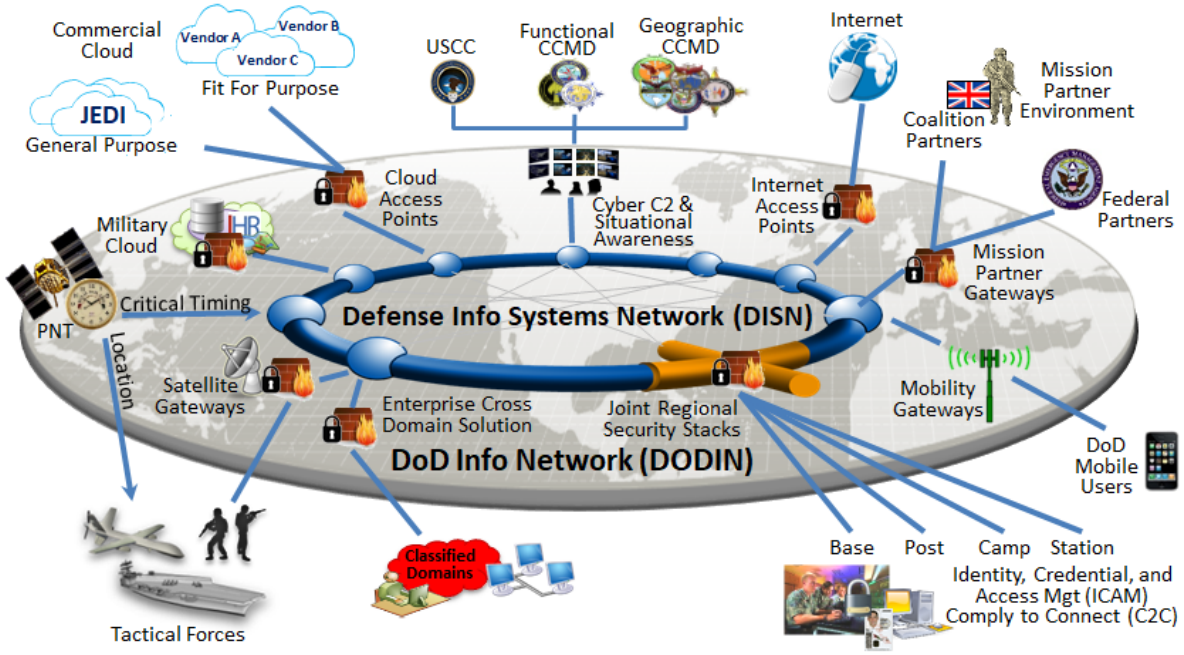


Figure 6: Scope of the JIE Framework

In addition to core infrastructure, the JIE also includes deployed tactical components that are designed to work with core JIE infrastructure and also operate autonomously, should connectivity to the core JIE be lost or denied. Due to the unique operating environments for these tactical JIE components, such as ships, aircraft, vehicles, etc., these components will be architected, designed, and developed by the individual Services to meet the mission operational and performance requirements of the tactical units.

The DoD CIO leads the development, integration, and synchronization of JIE management and oversight. The JIE Executive Committee (JIE EXCOM), a tri-chaired governance body at the Senior Executive Service/Flag Officer/General Officer (SES/FO/GO) level by the DoD CIO, the U.S. Cyber Command (USCYBERCOM), and the Joint Staff J6, sets the JIE direction, articulates goals and objectives, oversees the JIE Framework, and maintains accountability. The JIE EXCOM comprises stakeholders across the Department to provide oversight and approval of capability requirements, solutions, funding, and scheduling—ensuring that DoD Component expertise and insight in such areas as cybersecurity are incorporated in approaches and designs. The JIE EXCOM is focused on a more enterprise-wide approach, which couples centralized oversight with the ability to react to and anticipate the unique needs of the DoD Components. The priority of the IT and cyberspace capabilities in the JIE portfolio vary and therefore the JIE EXCOM is focused on those identified as high-level priorities.

The JIE EXCOM is the governance body that oversees the ten JIE Capability Objectives, and as such, approves any changes, additions, or deletions. The JIE EXCOM is supported by other subordinate bodies. Additionally, each Capability Objective has an established working group,

Integrated Product Team (IPT), or senior forum that reports to the JIE EXCOM so that existing working groups can be leveraged to address Capability Objective progress.

The table below illustrates how the JIE Capability Objectives and their associated initiatives align to DoD Digital Modernization Strategy objectives.

Table 1: Alignment of DoD CIO Objectives to JIE Capability Objectives and Initiatives

JIE Capability Objective	JIE Initiatives	DoD CIO Objectives
Modernize Network Infrastructure	Optical Transport Upgrades, MPLS Routers Buildout, ATM Switch and low speed TDM Circuit Elimination, Satellite Communications Gateway Consolidation and Modernization, IPv6 Implementation	• Modernize Warfighter C4 Infrastructure and Systems • Modernize DISN Transport Infrastructure • Modernize and Optimize DoD Component Networks and Services
Enable Enterprise Network Operations	Establish global and regional operations centers, Establish the JIE Management Network, Converge IT Service Management (ITSM) solutions	• Modernize and Optimize DoD Component Networks and Services • Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
Implement Regional Security	JRSS, JMS	• Modernize DISN Transport Infrastructure
Provide Mission Partner Environment (MPE)	Virtual Data Center, Applications and Services, MPE Transport, Mission Partner Gateways	• Strengthen Collaboration, International Partnerships, and Allied Interoperability
Optimize Data Center Infrastructure	Data Center Optimization Initiative (DCOI) and Application Rationalization Initiative	• Optimize DoD Data Centers
Implement Consistent Cybersecurity Protections	Enterprise Perimeter Protection Capabilities, Operate Securely in the Cloud, Endpoint Security, Data Center Security, Cyber Situational Awareness Analytic Capabilities (CSAAC)/ Big Data Platform (BDP), Identity, Credential, and Access Management (ICAM)	• Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Deploy an End-to-End ICAM Infrastructure
Enhance Enterprise Mobility	Purebred for Mobile, Defense Enterprise Mobility-Classified Consolidation, DoD Mobile Application Store, Pentagon Mobility	• Improve Information Sharing to Mobile Users

JIE Capability Objective	JIE Initiatives	DoD CIO Objectives
Standardize IT Commodity Management	Enterprise Software Agreements, Enterprise License Agreements, Enterprise Hardware Agreements, IT Asset Management, Windows 10 SHB Fourth Estate Network Optimization	• Improve IT Category Management • Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience
Establish End-User Enterprise Services	Enterprise Collaboration and Productivity Services	• Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
Provide Hybrid Cloud Computing Environments	Cloud Services	• Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)

The document entitled *Achieving the Joint Information Environment Vision*[8] provides more detail on the scope of the JIE Framework, including more information on initiatives supporting each of the Capability Objectives.

Information Technology (IT) Reform

DoD IT reform activities are a subset of JIE framework initiatives focused on realizing cost savings and gaining efficiencies throughout the Department. IT reform activities result in returned savings that can be reinvested to directly improve lethality, readiness, and operational capability. Reform activities will establish a consolidated and converged IT infrastructure to drive efficiencies across the Department. In addition, reform activities will provide opportunities for reductions in acquisition overhead, an increase in combined purchasing power, and the utilization of shared expertise across DoD. Finally, reform activities will standardize and modernize the digital environment to eliminate unnecessary systems and to allow DoD to focus finite cyberspace resources across fewer areas, ultimately shrinking the Department's cyberspace threat attack surface. Initial areas of execution include the following:

- ***Network and Service Optimization Reform*** - Converges DoD networks, service desks, and Network/Security Operations Centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives.
- ***Cloud and Data Center Optimization Reform*** - Transitions DoD to a cloud-enabled future, while leveraging commercial best practices, standardizing IT commodity

[8] The JIE portal is the repository for this document (https://intelshare.intelink.gov/sites/dodjie).

applications, and using commercial industry capabilities to deliver modernized services and warfighting capabilities.

- ***Enterprise Collaboration / IT Tools Reform*** - Converges and transitions DoD collaboration capabilities into a unified commercial cloud-enabled enterprise service.
- ***License Consolidation Reform*** - Negotiates improved terms and conditions with commercial vendors, prioritizes IT spend across the Department, and standardizes purchasing processes.

4 Cybersecurity

DoD's approach to cybersecurity is documented in the Cybersecurity Reference Architecture (CSRA).[9] The CSRA will allow for Command and Control, Situational Awareness, DCO-IDM, and an increased cybersecurity posture throughout the DODIN.

Security in the DoD cloud will be based on a holistic security architecture, providing for multi-cloud cybersecurity operations that include cloud native defenses, and which can adapt and respond to changing operational requirements. Existing DoD cloud security is accomplished by compliance with controls and security guidelines largely derived from security best practices for on-premises computing. To expand use of cloud, DoD will continually update controls and guidance, and also begin to adopt technologies and security operations that are inherently cloud native. Each cloud environment will continuously iterate to employ the latest cybersecurity technologies and methodologies to ensure the security of our information. Security will be automated to the maximum extent possible and leverage advanced cloud capabilities such as AI to provide high reliability and assurance without excessive cost or administrative burden.

The Department will extend and virtualize the DODIN boundary protection to operate securely in the cloud. Secure cloud operations will be achieved through on-going, integrated cybersecurity operations that support rapid incident response and predictive mitigations. Using common commercial cloud service providers and common services will enable increased reciprocity for security accreditations and thus reduce cloud migration times.

The result of implementing cybersecurity protections will be that:

- The DODIN—to include the data on the network—is defended as a virtual single information environment through common processes and capabilities.
- Cyberspace-defenses sense and respond to external and internal threats and take appropriate remediation, mitigation, and restoration actions.
- Command and control of the forces that operate on the DODIN is supported by shared cybersecurity situational awareness of the network as a whole.
- IT security findings are shared and reused throughout the Department to the greatest extent practical.
- DoD delivers an assured cloud computing environment capable of ensuring continued mission execution in the face of advanced persistent threats.
- Control Systems that underpin all aspects of the DoD Information Enterprise and operational assets are resilient to cyber exploitation

[9] The Warfighter Mission Assurance (WMA) portal is the repository for DoD architecture documents.

The remainder of this section covers the elements that comprise the DoD CSRA.

Enterprise Perimeter Protection

Enterprise Perimeter Protection (EPP) consolidates gateway security services, reducing cost and increasing security through centrally managed locations. The EPP establishes a protection barrier between the Internet, mission partner networks, and commercial cloud services, providing the ability to detect, inspect, block, and collect traffic in accordance with security policies. The EPP provides the foundation for routing Internet traffic through the Internet Access Point, routing mission partner traffic through the Mission Partner Gateway, routing Unclassified/Internet and Classified mobility end user traffic through the Mobility Gateway, and routing commercial cloud traffic through the Cloud Access Point to leverage shared enterprise cybersecurity components.

Mobile Endpoint Security

Since traditional endpoint security for Windows-based devices is not suitable for mobile devices, commercially available mobile security capabilities for Mobile Threat Defense and Security Enhanced Android Management must be deployed instead. As new commercially available mobile security technologies are developed to address growing threat vectors, these technologies will be assessed and deployed where applicable within DoD security guidelines.

Midpoint Security

The centerpiece of DoD's midpoint, or regional, security is the Joint Regional Security Stacks (JRSS). JRSS provides virtual network security that replaces or supplements the functionality of legacy network security systems operated by Combatant Commands, Services, and Agencies. In addition, JRSS shrinks the network's attack surface from a multitude of non-standard DoD Component-operated network security suites to approximately 50 standardized security suites that the Defense Information Systems Agency (DISA) and DoD Components operate and manage jointly. With JRSS, all traffic entering and leaving the Department's IP networks is examined for cybersecurity threats by JRSS's suite of sensors. In addition to local analysis, the resulting data are provided to the Department's broader analytic capability to enable enterprise-wide analysis for quicker, more effective responses to cybersecurity threats.

Enterprise Endpoint Security (including Windows 10 Secure Host Baseline)

Enterprise Endpoint Security is an integrated set of people, processes, and technology that work together to prevent unauthorized access to endpoints, identify and remove malicious code and unauthorized software, and prevent the execution of unauthorized software and processes. Endpoint Security leverages and integrates collaborative capabilities of DoD Components such as Comply to Connect (C2C) and containment, visibility, and assessment tools.

Additionally, Endpoint Security protects authorized platforms/devices that connect to the DODIN, allowing authorized users to obtain secure access to JIE resources from anywhere, at any time, using any authenticated device. The Department is standardizing across the enterprise on the Windows 10 SHB operating system, which will enable the Department to leverage

common applications and DoD-wide solutions, ensure quicker software patching, and configure all DoD computers to approved security standards, at a reduced lifecycle cost.

Data Security (for Data Centers and Cloud)

DoD is increasing data security by transitioning its data centers to a smaller number of improved Core Data Centers (CDCs) and Core Enterprise Data Centers (CEDCs). The consolidation of DoD-wide applications at CDCs and CEDCs provides consistent information protection with a centralized, advanced, and highly monitored security stack. All traffic flows into a CDC or CEDC are terminated and regenerated by proxy.

Big Data Platform (BDP)

The DoD's Big Data Platform (BDP) is a secure, extensible, scalable, agile, and open infrastructure platform designed to provide a distributed computing solution. The BDP is based on DISA-developed open source technologies and is capable of ingesting, storing, and visualizing multiple petabytes of data. It acts as a common platform that can support a variety of cyberspace missions and organizations across DoD. The BDP provides the ability to perform aggregation, correlation, historical trending, and forensic analysis against structured and unstructured data from a variety of systems and sensors supporting both NIPRNET and SIPRNET environments. The DODIN Operations and DCO missions require a capability that can translate enterprise scale data into simple, dynamic visualizations that depict event relationships and answer leaders' information requirements.

The Department intends to leverage a general data analytics capability to provide Enterprise situational awareness for DCO and DODIN Operations. This capability will enable the Department to:

- Have complete visibility of all sensor alerts and data flows end-to-end (Internet to host).
- Provide a common operational picture displaying DCO condition and vulnerability status.
- Understand missions affected by events captured by the sensors and report on system outages or attacks.
- Predict attacks based on historic trends and patterns.

Identity, Credential, and Access Management (ICAM)

The Department's approach to ICAM consists of four pillars:

- Digital Identity Management**:** Establishment of the digital identity and lifecycle management.
- Credential Management: Issuing of a physical or electronic token (Common Access Card (CAC)/Public Key Infrastructure (PKI) Cert and/or Account) as a proxy for an entity's authoritative digital identity.
- Authentication: Assertion of identity via a credential and validation of that credential as genuine. PKI is the DoD's current technological solution to authentication. However,

approved multi-factor authentication and identity federation services are available when PKI cannot be used.

- Authorization: Approving access based on digital policies and authoritative information about requesting identities and the resource being accessed.

Under this approach to ICAM, all access decisions are based on identity information from an authoritative source, and those decisions are dynamically configurable to support changing mission needs, attack responses, and system degradations. In addition, audits support real-time and historical forensic activity.

Appendix A: Technologies Offering Promise to DoD

Looking toward the future, the Department is exploring a number of technologies that have the promise to provide increased effectiveness, efficiency, and security. Representative technologies include AI, Big Data Analytics, Evergreen IT approaches, DevSecOps, Hyper-Converged Infrastructure, Serverless or Event-Driven Computing, Software Defined Networking (SDN), Block Chain, Cryptographic Modernization, Quantum Computing, Internet of Things (IoT), 5G, Internet Protocol version 6 (IPv6), Passive Optical Network (PON), and Zero Trust Security. These technologies are briefly described below, along with discussion of how each technology might increase the Department's effectiveness, efficiency, and security. A number of these technologies can work together to provide the Department with the potential for quantum leaps in capability.

Artificial Intelligence (AI)

Artificial Intelligence refers to the ability of machines to perform tasks that normally require human intelligence—recognizing patterns, learning from experience, drawing conclusions, making predictions, taking action, and more—whether digitally or as the smart software behind autonomous physical systems. As a general purpose enabling technology, much like electricity, computers, or networks, AI is already transforming large segments of businesses and industries and is expected to impact every corner of the DoD including force application, force protection, training, logistics, C4ISR, cyberspace operations, back-office business functions and more. With the application of AI to defense, we have an opportunity to improve support for and protection of U.S. service members, safeguard our citizens, defend our allies and partners, and improve the affordability and speed of our operations.

The military competitor who can harness and exploit AI's potential the fastest will accrue a significant military advantage. The Department must shape this emerging military-technical competition in AI to our advantage while ensuring a strong commitment to military ethics and AI safety. Decisive warfighting advantage in this new competitive era will go to those who integrate and adapt leading-edge technology to create innovative operational concepts with speed and agility. Realizing the DoD's AI Strategy requires identifying appropriate use cases for AI across DoD, rapidly piloting solutions, and scaling successes across the enterprise. The Joint AI Center (JAIC) is the focal point for carrying out the Strategy.

Big Data Analytics

DoD's approach to Big Data Analytics is based upon a Big Data Platform (BDP), a secure, extensible, scalable, agile, and open infrastructure platform designed to provide a distributed computing solution. BDP instances are capable of ingesting, storing, and visualizing multiple petabytes of data from a variety of sources (e.g., mobile devices, aerial (remote) sensing, software logs, cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks).

Big Data Analytics applications enable analysis of volumes of structured data, plus other forms of data (semi-structured and unstructured) that are often left untapped by conventional business intelligence (BI) and analytics programs. Data mining tools sift through data sets in search of patterns and relationships enabling aggregation, correlation, historical trending, and forensic analysis against the data. Machine learning algorithms can analyze large data sets and perform deep learning, a more advanced offshoot of machine learning to support predictive analytics that forecast behavior and other future developments.

Evergreen IT Approaches

Evergreen IT is the perpetual updating of end-user software, hardware, and associated services such as mailboxes, telephony, file storage, and the infrastructure supporting the technology. It requires a combination of people, process, and technology to deliver optimal results. It involves a budgetary and executive commitment to ensuring that no end-user technology is ever more than N-x (x to be defined by each organization) behind the currently available version within a pre-determined timeframe.

Evergreen IT encompasses not only the services at the user level but all of the underlying infrastructures, whether on-site or outsourced. Many organizations believe that Evergreen IT holds promise for reducing the resources and energy they need to expend on providing the up-to-date and flexible services that their users are demanding.

For hardware, it means that every piece of physical equipment is kept within warranty or lease and is refreshed on a fixed timeline. The process means that the organizational processes are in place for procurement, licensing, scheduling, communications, and deployment, and that the process is highly repeatable. To achieve this, creating a set of tasks that are repeatable and in constant use will be vital.

A particular benefit of this approach is that a real-time understanding of the IT environment and its currency is always available, and that for all hardware or software outside of defined evergreen thresholds, a project is running to perform the upgrade.[10]

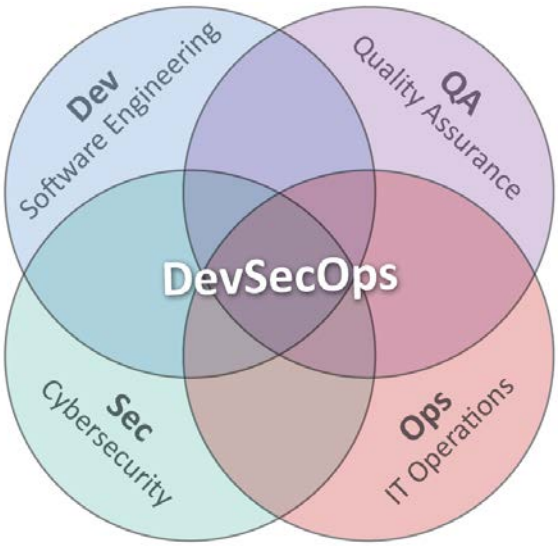
DevSecOps

Over the last decade and a half, Agile approaches to software development and systems engineering have demonstrated their ability to lower costs, improve quality and customer satisfaction, and reduce time to delivery. Such benefits are particularly realized when Agile approaches are carried out in a disciplined manner that extends to collaboration between IT development, security, and IT operations, or DevSecOps. Such an approach also ensures that Quality Assurance (QA) and Cybersecurity are included in the collaboration, as shown in Figure 7.

[10] Text in this section adapted from: https://blog.juriba.com/evergreen-it-concept-or-reality

DevSecOps is the natural extension of Agile methods and encompasses the tools, services, and standards that enable IT development, security, and operations disciplines to come together in the development, deployment, and operation of applications in a secure, flexible, and interoperable fashion. DevSecOps emerged from a much-expanded understanding of the value of collaboration between development and operations staff in an increasingly contested environment —which historically functioned in relative siloes—throughout all stages of creating and operating a service, and how important security and operations have become in our increasingly service-oriented world. DevSecOps is a set of practices that automates the processes between software development and IT teams, in order to build, test, and release software faster, more reliably, and more securely.

Figure 7: DevSecOps Ties Key Disciplines Together



By having all key areas together, the rapid release cycles of the Agile process can be accommodated by the more traditional disciplines of IT.

DevSecOps increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. This speed enables organizations to better serve their customers.

Hyper-Converged Infrastructure (HCI)

Hyper-convergence is a type of infrastructure approach that is largely software-defined with tightly-integrated compute, storage, networking, and virtualization resources running on commodity hardware. This stands in contrast to a traditional converged infrastructure, where each of these resources is typically handled by a discrete hardware component that serves a singular purpose.

HCI dramatically improves server availability and performance as well as storage scalability since it is no longer limited to locally attached disks. Software-defined storage (SDS) technology aggregates all existing hard drives within a cluster and represents them as a single, highly available, highly redundant storage capacity pool. Using this approach, if one disk or node goes down, data is still available for the rest of the cluster, so workloads will continue running on top of remaining nodes without disruption.

HCI enables a shift in management paradigm from a hardware approach to an application-focused one, with centralized management, policies, and mobility conducted at the virtual machine level. HCI's flexible infrastructure makes it easier to launch new cloud services, to

support enterprises that want to easily package and migrate new workloads. HCI enables operations to scale up quickly to meet new demands without disrupting existing applications. Simply put, HCI focuses on the user and helps cut down deployment of new services to the user to a matter of minutes.

Optimizing infrastructure costs is another major appeal of HCI, which can drive better performance while at the same time reducing Total Cost of Ownership. Savings are expected to result from streamlined acquisition and deployment; lower management, operations, and support costs; as well as reduced complexity and fewer interoperability issues. According to International Data Corporation (IDC), HCI delivers a 65 percent reduction in storage-related capital expenditures and a 50 percent reduction in total cost of ownership.[11]

Serverless, or Event-Driven, Computing

Serverless, or event-driven, computing is a cloud service that executes specific functions, such as image processing and database updates. Traditional cloud deployments require users to establish a compute instance and load code into that instance. Then, the user decides how long to run—and pay for—that instance. With serverless computing, developers simply create code, and the cloud provider loads and executes that code in response to real-world events, so users don't have to worry about the server or instance aspect of the cloud deployment. Users only pay for the number of transactions that the function executes. Serverless computing services are already available from major commercial cloud service providers.[12]

Software Defined Networking (SDN)

Software defined networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center. In a software-defined network, a network administrator can shape traffic from a centralized control console without having to touch individual switches, and can deliver services to wherever they are needed in the network, without regard to what specific devices a server or other hardware components are connected to. The key technologies for SDN implementation are functional separation, network virtualization, and automation through programmability.

Under SDN, rules for packet handling are sent to switches from a controller, an application running on a server somewhere, and switches query the controller for guidance as needed, and provide it with information about the traffic they are handling. A system administrator can change any network switch's rules when necessary—prioritizing, de-prioritizing, or even blocking specific types of packets with a very granular level of control. This is especially helpful in a cloud computing multi-tenant architecture, because it allows the administrator to manage

[11] http://www.multipolar.com/file_upload/downloads/7203-VSAN-0148_IDC_Current_State_of_HCI_and_Benefits_of_vSAN.PDF
[12] Content for this topic adapted from material at this URL: https://searchcloudcomputing.techtarget.com/definition/cloud-computing

traffic loads in a flexible and more efficient manner. Essentially, this allows the administrator to use less expensive commodity switches and have more control over network traffic flow than ever before.[13]

Block Chain Cybersecurity Shield

Blockchains are a new information technology that inverts the cybersecurity paradigm. First, blockchain networks are trustless: they assume compromise of the network by both insiders and outsiders. Second, blockchains are transparently secure: they do not rely on failure-prone secrets, but rather on a cryptographic data structure that makes tampering both exceptionally difficult and immediately obvious. Finally, blockchain networks are fault tolerant: they align the efforts of honest nodes to reject those that are dishonest. As a result, blockchain networks not only reduce the probability of compromise, but also impose significantly greater costs on an adversary to achieve it.

The Defense Advanced Research Projects Agency (DARPA) is starting to experiment with blockchain to create a more efficient, robust, and secure platform using a blockchain protocol that will allow personnel from anywhere to transmit secure messages or process transactions that can be traced through numerous channels of a decentralized ledger. The application will be used in different ways, including facilitating communication between units and headquarters, and transmitting information between intelligence officers and the Pentagon. DARPA also has been trying to develop an unhackable code—which blockchain could facilitate—because the technology offers intelligence on hackers who try to break into secure databases.

Cryptographic Modernization

The objective of Cryptographic Modernization (CM) is to ensure an appropriate security posture for national security systems by providing transparent cryptographic capabilities consistent with operational imperatives and mission environments.[14]

Underway since 2000, CM replaces U.S. and allied equipment reaching the end of useful cryptographic life with modern capabilities. Initial priorities included retirement of 20-30+ years old technologies, transition from point-to-point to network-centric cryptographic systems, and countermeasure actions in response to continued advances in computer processing power which enhanced adversary capabilities against DoD systems. These factors necessitate re-engineering or replacement of most fielded equipment. DoD and the National Security Agency (NSA) are now preparing for Cryptographic Modernization 2 (CM2). CM2 will ensure the Department stays well ahead of operational vulnerabilities and emerging threats, such as quantum computing. It continues replacement of aging equipment and assures modernization of our cryptographic capabilities to meet warfighter needs well into the 2030s.

[13] Text in this section adapted from: http://searchsdn.techtarget.com/definition/software-defined-networking-SDN
[14] http://csla.army.mil/Sections/Cryptomod/cryptomod.aspx

Quantum Computing[15]

Quantum computing involves harnessing and exploiting the laws of quantum mechanics to process information. Whereas a traditional computer uses long strings of bits, which encode either a zero or a one, a quantum computer uses quantum bits, or qubits. Quantum computing, once engineered, will be a disruptive technology due to the unique capabilities that quantum mechanics provide. Of interest to DoD are the properties which enable qubits to remain correlated over great distances, with potential communications applications, and the ability to process a vast number of calculations simultaneously. These features give a quantum computer the potential to be millions of times more powerful than today's most powerful supercomputers and to quickly and efficiently solve difficult tasks that have been thought impossible for classical computers, such as factoring very large numbers.

The Department will seize opportunities to advance and implement quantum computing capabilities for military purposes and recognizes that our adversaries can use those same capabilities. To address the emerging threat, the Department is pursuing modernization initiatives that, when implemented, ensure the protection of critical DoD information and systems.

Internet of Things (IoT)

IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to its user, but it is now connected to surrounding objects and database data. The assortment of embedded sensors and connected devices that comprise IoT enables technology to gain the ability to sense, predict, and respond to our needs and can be integrated into our decision-making processes and natural behaviors. Accordingly, the Department can use computers to gather and use data from these objects—to enable tracking, counting and analyzing in order to greatly reduce waste, loss, and cost. DoD managers would know when things needed replacing, repairing, or recalling, and whether they were fresh or past their best.

5G

5G is the next generation of mobile network technologies. 5G (also known as 5G New Radio (5G NR)) encompasses wireless standards, emerging technologies, and mobile platform delivery services designed to deliver enhanced mobile broadband and machine to machine communications. 5G NR holds the promise of delivering new levels of wireless network performance, capabilities, and efficiencies for the Department. Key benefits from 5G NR are the ability to deliver fiber-like speeds to end-user devices, improved performance at network cell edge, low latency performance (<2ms radio latency), and greater spectral efficiency. Foundational technologies include: improved beamforming via smart antennas, network

[15] Material in this section is based on content from these sites: https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101 and https://computer.howstuffworks.com/quantum-computer1.htm

densification via small cells, native support for diverse spectrum types (licensed and unlicensed), and increased network intelligence via software defined networking (SDN).

Some near-term implications for 5G include an evaluation of potential supply chain risk from foreign vendors controlling 5G SDN components and monitoring for the development of "trusted" and "assured" 5G networks that do not inherit vulnerabilities from 2G, 3G, or 4G networks. The CIO will also evaluate whether new spectrum policy is required, should 5G global spectral harmonization efforts require DoD to move from primary to co-primary or secondary status, resulting in a net loss of spectrum access capability.

Further in the future, as 5G operations become widespread, DoD's wireless carrier contracts will need to be updated for additional services and higher data rates. 5G's extensive use of virtualization will permit "network slice" applications that are tailored for specific DoD missions. Potential applications include NLCC National Security networking, IoT base surveillance/perimeter security and base/post private communication networks. Overall, 5G will support improved bandwidth at DoD U.S. locations.

Internet Protocol version 6 (IPv6)

IPv6 implementation is a strategic priority for the Department. Growing internal demand, accelerating global and mission partner adoption, increasing reliance on commercial solutions and services, emerging technology and standards, and business trends necessitate renewed focus. A proactive approach is essential as significant work remains. The gaining the necessary experience and completing the people, process and technology preparations to enable secure and reliable IPv6 services in support of DoD missions will take time.

The Internet is now effectively bi-lingual with both IPv4 and IPv6 widely used. The mobile ecosystem, Internet Service Providers, computer manufacturers and Internet content providers lead the way, but other technology providers are now establishing their IPv6 strategies. Total IPv4 address space is not sufficient for the expected demand from convergence on IP (Everything over IP) and continued growth of the Internet, mobility, cloud computing and IoT. Gartner estimates the number of connected devices will exceed 20 billion by 2020. Recognizing this, the Internet Architecture Board advised standards development organizations in 2016 to begin optimizing for IPv6. Additionally, emerging technologies of DoD interest, such as smart infrastructure, cloud services and automotive Ethernet, are leveraging IPv6 and will expand its applications. In particular, 5G will be enabled and operationalized through IPv6. As a result, many of our mission partners and strategic competitors are preparing for an IPv6-centric future. Notably, at the end of 2017, China announced its goal, by the end of 2025, to establish the world's largest IPv6 network in terms of network scale, quantity of users, and network traffic volume.

IPv6 also provides performance benefits, management efficiencies, and support for new capabilities and services. For example, IPv6 reduces the size of routing tables and makes routing

more efficient and hierarchical. Additionally, its simplified packet header makes packet processing more efficient. It also provides expanded address space, eliminates address conflict issues common under IPv4, simplifies network mergers, enables more streamlined connections, and as a result can improve user experience.

Passive Optical Network (PON)

A passive optical network is a form of fiber-optic access network that implements a point-to-multipoint architecture, in which unpowered fiber optic splitters are used to enable a single optical fiber to serve multiple end-points. Therefore, PON requires far less infrastructure since it reduces the amount of fiber and central office equipment required, compared with point-to-point architectures.

The main benefits of PON are listed below:

- Lower network operational and maintenance costs
- Lower infrastructure costs
- Large bundles of copper cable are replaced with small, single mode optical fiber cable
- PON provides increased distance between data center and desktop (>20 kilometers)
- Fiber is more secure than copper; it is harder to tap

Zero Trust Security

Zero Trust Security is an emerging initiative that DoD CIO is exploring in concert with DISA, US Cyber Command (USCYBERCOM), and the NSA. Zero trust is a cybersecurity strategy that embeds security throughout the architecture for the purpose of stopping data breaches. This data-centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi-attribute based confidence levels that enable authentication and authorization policies under the concept of least privileged access. Implementing zero trust requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way while enabling unimpeded operations.

While straightforward in principle, the actual implementation and operationalization of zero trust has significant complexity in areas that include network configuration, software defined networking, data tagging, analytics, access control, policy orchestration, encryption, and automation, as well as end-to-end identity, credential, and access management (ICAM). Enterprise level considerations include identifying which data, applications, assets, and services to protect, and mapping transaction flows, policy decisions, and locations of policy enforcement. Apart from the advantages to securing our architecture in general, there are additional cross-functional benefits.

Cloud deployments are excellent candidates for implementing zero trust concepts, especially when using commercial clouds. If the cloud infrastructure itself is ever compromised, a zero trust compliant architecture provides protection from adversaries seeking to entrench themselves in

our virtual network. While commercial clouds offer an excellent opportunity to scale capability and control costs, they pose risks since we do not control the infrastructure and there may be delays in communicating compromises. The assumption zero trust makes—that you are compromised—is particularly suited to cloud infrastructures.

Security automation and orchestration is a critical capability for successfully deploying and managing a zero trust compliant infrastructure. The additional authentication, authorization, monitoring, and analytical requirements can no longer be managed manually. For example, secure credentialing of all nodes requires an automation capability that ensures keying and rekeying happens at machine speed and isn't delayed by unnecessary human intervention. This requires authenticated and authorized devices being assured that the devices they are communicating with are healthy and approved (device attestation).

Cryptographic modernization will be needed to ensure that data is protected at a level compliant with the Commercial National Security Algorithm (CNSA) suite as defined in Committee on National Security Systems (CNSS) Policy 15. This upgrade of the cryptographic security of our systems can pose significant challenges to legacy applications and hardware that can vary significantly in how they support the larger key sizes and algorithms required.

Analytics will need additional capability to handle the required sensor and logging data associated with zero trust security. Different processes and procedures may need to be incorporated to measure the health of the network and identify anomalous behavior. For example, end-to-end encryption between internal resources on the network will limit the ability of internal packet inspection (lateral Break and Inspect) to detect problems. New analytical measures will need to be employed to ensure that only authorized communication is taking place.

Microelectronics

Microelectronics is a foundational technology to Digital Modernization thrusts. The Department is faced with the dual problems in microelectronics of low market share and an expansive range of needs, from boutique and legacy components to state of the art technologies. Advanced microelectronics technology is essential for modernization of current and next generation defense capabilities. Strategic goals, investments, and deliberate actions by strategic competitors threaten the Department's access to, and assurance of, the microelectronics supply that underpins our defense capabilities. The Department, aligned with other U.S. Government partners, is intent on reversing the trends through a whole-of-nation effort, fostering commercial and government alliances to preserve the U.S. semiconductor and microelectronics ecosystem, lower barriers to innovation and adoption, strengthen workforce expertise, lead the next generation of advanced technology, and maintain the U.S. as the global source for high-end, secure and reliable microelectronics components.

Appendix B: Alignment to DoD Strategic Guidance

The DoD Digital Modernization Strategy presents the Department's IRM-related strategic goals and objectives, which demonstrate the DoD CIO's support of the Secretary of Defense's goals, priorities and objectives found in the DoD National Defense Business Operations Plan, as well as in the President's National Security Strategy, the Department's National Defense Strategy, the Chairman of the Joint Chiefs of Staff's National Military Strategy, and the Defense Planning Guidance, along with legislative guidance and direction contained in National Defense Authorization Acts. In addition, the DoD Digital Modernization Strategy supports the goals contained in the DoD IT Reform Memo.

2018 National Defense Business Operations Plan

The DoD CIO goals and objectives (described in Section 2) provide direct support for the Secretary's DoD Strategic Goals:

- Goal #1: Rebuilding Military Readiness as We Build a More Lethal Joint Force
- Goal #2: Strengthen Our Alliances & Attract New Partners
- Goal #3: Reform the Department's Business Practices for Greater Performance and Affordability

The table below provides a summary view of the DoD CIO goals and objectives that support each DoD Strategic Goal and Strategic Objective:

Table 2: Alignment of DoD CIO Objectives to Department Strategic Goals and Objectives

DoD Strategic Goal	DoD Strategic Objective	DoD CIO Goal	DoD CIO Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.2: Lay the foundation for future readiness through recapitalization, innovation, and modernization	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems • Treat Data as a Strategic Asset • Strengthen Collaboration, International Partnerships & Allied Interoperability • Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity • Enhance the Delivery and Protection of PNT • Modernize Defense Information Systems Network (DISN) Transport Infrastructure

DoD Strategic Goal	DoD Strategic Objective	DoD CIO Goal	DoD CIO Objectives
			• Modernize and Optimize DoD Component Networks and Services • Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport • Improve Information Sharing to Mobile Users • Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO) • Drive Standards into DoD IT Systems
		Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3) • Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience • Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure

DoD Strategic Goal	DoD Strategic Objective	DoD CIO Goal	DoD CIO Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.3: Enhance information technology and cybersecurity capabilities	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Treat Data as a Strategic Asset • Strengthen Collaboration, International Partnerships & Allied Interoperability • Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity • Enhance the Delivery and Protection of PNT • Modernize Defense Information Systems Network (DISN) Transport Infrastructure • Modernize and Optimize DoD Component Networks and Services • Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport • Improve Information Sharing to Mobile Users
		Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3) • Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience • Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure • Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems • Reform DoD Cybersecurity Risk Management Policies and Practices

DoD Strategic Goal	DoD Strategic Objective	DoD CIO Goal	DoD CIO Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.4 Ensure the best intelligence, counterintelligence, and security support to DoD operations	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems • Treat Data as a Strategic Asset • Modernize DISN Transport Infrastructure • Modernize and Optimize DoD Component Networks and Services • Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport • Improve Information Sharing to Mobile Users • Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO) • Drive Standards into DoD IT Systems
		Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience • Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure • Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems • Reform DoD Cybersecurity Risk Management Policies and Practices
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.5 Implement initiatives to recruit and retain the best total force to bolster capabilities and readiness	Cultivate Talent for a Ready Digital Workforce	• Strengthen the Cyber Functional Community Workforce • Strengthen the IT Acquisition Workforce • Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development

DoD Strategic Goal	DoD Strategic Objective	DoD CIO Goal	DoD CIO Objectives
#2: Strengthen Our Alliances & Attract New Partners		Innovate for Competitive Advantage	• Strengthen Collaboration, International Partnerships & Allied Interoperability
		Optimize for Efficiencies and Improved Capability	• Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems
#3: Reform the Department's Business Practices for Greater Performance and Affordability	3.1: Improve and strengthen business operations through a move to DoD-enterprise or shared services; reduce administrative and regulatory burden	Innovate for Competitive Advantage	• Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
		Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3) • Improve IT Category Management • Improve Rapid Technology Deployment Processes • Strengthen IT Financial Management Decision Making and Accountability
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems • Reform DoD Cybersecurity Risk Management Policies and Practices
#3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3 Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Optimize for Efficiencies and Improved Capability	• Strengthen IT Financial Management Decision Making and Accountability

Appendix C: Alignment with the President's Management Agenda

The table below shows how different DoD CIO goals and objectives align with and support the fourteen (14) Cross Agency Priority Goals of the President's Management Agenda.

Table 3: Alignment of DoD CIO Objectives to the President's Management Agenda

President's Management Agenda	DoD CIO Goal	DoD CIO Objectives
Cross Agency Priority Goal #1: Modernize IT to increase productivity and security	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems • Treat Data as a Strategic Asset • Strengthen Collaboration, International Partnerships & Allied Interoperability • Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity • Enhance the Delivery and Protection of PNT • Modernize Defense Information Systems Network (DISN) Transport Infrastructure • Modernize and Optimize DoD Component Networks and Services • Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport • Improve Information Sharing to Mobile Users • Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO) • Drive Standards into DoD IT Systems
	Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3) • Improve Rapid Technology Deployment Processes

President's Management Agenda	DoD CIO Goal	DoD CIO Objectives
	Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience • Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure
Cross Agency Priority Goal #2: Leveraging Data as a Strategic Asset	Innovate for Competitive Advantage	• Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Treat Data as a Strategic Asset • Strengthen Collaboration, International Partnerships & Allied Interoperability • Modernize Defense Information Systems Network (DISN) Transport Infrastructure • Provide End-to-End Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Data Transport • Improve Information Sharing to Mobile Users • Drive Standards into DoD IT Systems
	Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Strengthen IT Financial Management Decision Making and Accountability
	Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure
Cross Agency Priority Goal #3: Developing a workforce for the 21st century	Cultivate Talent for a Ready Digital Workforce	• Strengthen the Cyber Functional Community Workforce • Strengthen the IT Acquisition Workforce • Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development
Cross Agency Priority Goal #4: Improving customer experience with federal services	Innovate for Competitive Advantage	• Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Strengthen Collaboration, International Partnerships & Allied Interoperability • Improve Information Sharing to Mobile Users
	Optimize for Efficiencies and Improved Capability	• Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)

President's Management Agenda	DoD CIO Goal	DoD CIO Objectives
		• Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
	Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure
Cross Agency Priority Goal #5: Sharing Quality Services	Innovate for Competitive Advantage	• Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
	Optimize for Efficiencies and Improved Capability	• Optimize DoD Data Centers • Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3) • Improve IT Category Management
Cross Agency Priority Goal #6: Shifting from low-value to high-value work	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation • Innovations at the Strategy Element level that will support high-value work: o Implement Software Defined Networking (SDN)
	Optimize for Efficiencies and Improved Capability	• Shift from Component-Centric to Enterprise-Wide Operations and Defense Model • Optimize DoD Data Centers • Improve Rapid Technology Deployment Processes
	Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Reform DoD Cybersecurity Risk Management Policies and Practices • Innovations at the Strategy Element level that will support high-value work: o Enhance Cybersecurity Situational Awareness through Big Data Analytics o Explore Cybersecurity Application of Blockchain Technology o Evolve Crypto Modernization
Cross Agency Priority Goal #7: Category Management – Leveraging Common Contracts and Best Practices to Drive Savings and Efficiencies	Optimize for Efficiencies and Improved Capability	• Improve IT Category Management

President's Management Agenda	DoD CIO Goal	DoD CIO Objectives
Cross Agency Priority Goal #8: Results-Oriented Accountability for Grants	N/A	
Cross Agency Priority Goal #9: Getting Payments Right	Optimize for Efficiencies and Improved Capability	• Strengthen IT Financial Management Decision Making and Accountability
Cross Agency Priority Goal #10: Improving Outcomes through Federal IT Spending Transparency	Optimize for Efficiencies and Improved Capability	• Strengthen IT Financial Management Decision Making and Accountability
Cross Agency Priority Goal #11: Improve Management of Major Acquisitions	Optimize for Efficiencies and Improved Capability	• Improve Rapid Technology Deployment Processes
	Cultivate Talent for a Ready Digital Workforce	• Strengthen the IT Acquisition Workforce
Cross Agency Priority Goal #12: Modernize Infrastructure Permitting	N/A	
Cross Agency Priority Goal #13: Security Clearance, Suitability, and Credentialing Reform	Evolve Cybersecurity for an Agile and Resilient Defense Posture	• Deploy an End-to-End Identity, Credential, & Access Management (ICAM) Infrastructure
Cross Agency Priority Goal #14: Improve Transfers of Federally-Funded Technologies from Lab-to-Market	Innovate for Competitive Advantage	• Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale • Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
	Optimize for Efficiencies and Improved Capability	• Improve Rapid Technology Deployment Processes

Appendix D: Alignment with DoD IT Reform Initiatives

The table below shows how different DoD CIO goals and objectives align with and support the DoD CIO-developed IT Reform Initiatives. Note that these DoD IT Reform Initiatives closely align with several Capability Objectives and associated modernization initiatives in the JIE Framework.

Table 4: Alignment of DoD CIO Objectives to DoD IT Reform Initiatives

DoD IT Reform Initiative	DoD CIO Goal	DoD CIO Objectives
Network and Service Optimization	Innovate for Competitive Advantage	• Modernize Defense Information Systems Network (DISN) Transport Infrastructure • Modernize and Optimize DoD Component Networks and Services
Cloud and Data Center Optimization	Innovate for Competitive Advantage	• Optimize DoD Data Centers • Deliver a DoD Enterprise Cloud Environment
Enterprise Collaboration / IT Tools	Optimize for Efficiencies and Improved Capability	• Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) • Optimize DoD Voice and Video Capabilities (ECAPS Capability Sets 2 & 3)
License Consolidation	Optimize for Efficiencies and Improved Capability	• Improve IT Category Management

Appendix E: DoD CIO Authorities

The DoD CIO is positioned with appropriate responsibilities and authorities to improve operating efficiency, encompass portfolio and program management, and focus on delivering IT solutions that support the Department's mission and business activities in a secure and efficient manner. The Department's federated management model integrates and balances CIO authorities with the additional specific DoD CIO authorities contained with Title 10, Title 40, and Title 44 in a manner that achieves the desired outcomes of operational efficiencies.

The fundamental DoD CIO statutory mandates are outlined in the table below:

Table 5: CIO Statutory Mandates

Authoritative Source	Mandates
Title 10 U.S.C. 142	• Chief Information Officer (a) There is a Chief Information Officer of the Department of Defense, who shall be appointed by the President, by and with the advice and consent of the Senate, from among civilians who are qualified to serve as such officer. (b) (1) The Chief Information Officer of the Department of Defense- (A) is the Chief Information Officer of the Department of Defense for the purposes of sections 3506(a)(2) (other than with respect to business systems and management) and 3544(a)(3) of title 44; (B) has the responsibilities and duties specified in sections 11315 and 11319 of title 40 (other than with respect to business systems and management); (C) has the responsibilities specified for the Chief Information Officer in sections 2223(a) (other than with respect to business systems and management) and 2224 of this title; (D) exercises authority, direction, and control over the Information Assurance Directorate of the National Security Agency; (E) exercises authority, direction, and control over the Defense Information Systems Agency, or any successor organization; (F) has the responsibilities for policy, oversight, guidance, and coordination for all Department of Defense matters related to electromagnetic spectrum, including coordination with other Federal and industry agencies, coordination for classified programs, and in coordination with the Under Secretary for Personnel and Readiness, policies related to spectrum management workforce; (G) has the responsibilities for policy, oversight, guidance, and coordination for nuclear command and control systems; (H) has the responsibilities for policy, oversight, and guidance for matters related to precision navigation and timing; and (I) has the responsibilities for policy, oversight, and guidance for the architecture and programs related to the information technology, networking, information assurance, cybersecurity, and cyber capability architectures of the Department.

Authoritative Source	Mandates
	(2) (A) The Secretary of Defense, acting through the Under Secretary of Defense (Comptroller), shall require the Secretaries of the military departments and the heads of the Defense Agencies with responsibilities associated with any activity specified in paragraph (1) to transmit the proposed budget for such activities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of this title [10 USCS § 221] for that fiscal year to the Chief Information Officer for review under subparagraph (B) before submitting the proposed budget to the Under Secretary of Defense (Comptroller). (B) The Chief Information Officer shall review each proposed budget transmitted under subparagraph (A) and, not later than January 31 of the year preceding the fiscal year for which the budget is proposed, shall submit to the Secretary of Defense a report containing the comments of the Chief Information Officer with respect to all such proposed budgets, together with the certification of the Chief Information Officer regarding whether each proposed budget is adequate. (C) Not later than March 31 of each year, the Secretary of Defense shall submit to Congress a report specifying each proposed budget contained in the most-recent report submitted under subparagraph (B) that the Chief Information Officer did not certify to be adequate. The report of the Secretary shall include the following matters: i. A discussion of the actions that the Secretary proposes to take, together with any recommended legislation that the Secretary considers appropriate, to address the inadequacy of the proposed budgets specified in the report. ii. Any additional comments that the Secretary considers appropriate regarding the inadequacy of the proposed budgets. (3) (A) The Secretary of a military department or head of a Defense Agency may not develop or procure information technology (as defined in section 11101 of title 40 [40 USCS § 11101]) that does not fully comply with such standards as the Chief Information Officer may establish. (B) The Chief Information Officer shall implement and enforce a process for-- i. developing, adopting, or publishing standards for information technology, networking, or cyber capabilities to which any military department or defense agency would need to adhere in order to run such capabilities on defense networks; and ii. certifying on a regular and ongoing basis that any capabilities being developed or procured meets such standards as have been published by the Department at the time of certification.

Authoritative Source	Mandates
	(C) The Chief Information Officer shall identify gaps in standards and mitigation plans for operating in the absence of acceptable standards. (4) The Chief Information Officer shall perform such additional duties and exercise such powers as the Secretary of Defense may prescribe. (c) The Chief Information Officer of the Department of Defense shall report directly to the Secretary of Defense in the performance of duties under this section. (d) The Chief Information Officer takes precedence in the Department of Defense with the officials serving in positions specified in section 131(b)(4) of this title. The officials serving in positions specified in such section and the Chief Information Officer of the Department of Defense take precedence among themselves in the order prescribed by the Secretary of Defense.
Title 10 U.S.C. 2222	• The Chief Information Officer of the Department of Defense shall develop an information technology enterprise architecture. The architecture shall describe a plan for improving the information technology and computing infrastructure of the Department of Defense, including for each of the major business processes conducted by the Department of Defense. • The Secretary shall establish a Defense Business Council to provide advice to the Secretary on developing the defense business enterprise architecture, reengineering the Department's business processes, developing and deploying defense business systems, and developing requirements for defense business systems. The Council shall be chaired by the Chief Management Officer and the Chief Information Officer of the Department of Defense. • Issuance of Guidance o Supporting guidance.-The Secretary shall direct the Chief Management Officer of the Department of Defense, the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Chief Information Officer, and the Chief Management Officer of each of the military departments to issue and maintain supporting guidance, as appropriate and within their respective areas of responsibility, for the guidance of the Secretary issued under paragraph (1).

Authoritative Source	Mandates
Title 10 U.S.C. 2223	In addition to the responsibilities provided for in chapter 35 of Title 44 and in section 11315 of Title 40, the Chief Information Officer of the Department of Defense shall— (1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems; (2) ensure the interoperability of information technology and national security systems throughout the Department of Defense; (3) ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed; (4) provide for the elimination of duplicate information technology and national security systems within and between the military departments and Defense Agencies; and (5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

Authoritative Source	Mandates
Title 10 U.S.C. 2224	The Secretary of Defense shall carry out a program, to be known as the "Defense Information Assurance Program", to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis. The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure. In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following: (1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces. (2) Development of essential information assurances technologies and programs. (3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare. (4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure. (5) The conduct of exercises, war games, simulations, experiments, and other activities designed to prepare the Department to respond to information warfare threats. (6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.
Clinger-Cohen Act of 1996 (CCA) (Title 40 U.S.C.)	• Establishes additional statutory responsibilities of agency CIOs • Responsibilities include: 1) IT architecture 2) Promote efficient design & operation of major Information Resources Management (IRM) processes, including improvement to agency work processes (business process reengineering) 3) Evaluate the performance of IT investments and advise agency head whether to continue, modify or terminate • Develop, maintain, and facilitate the implementation of a sound, secure, and integrated IT architecture
Paperwork Reduction Act (Title 44 U.S.C., Chapter 35, subchapter I)	• Establishes the position of the Agency CIO • Carry out DoD IRM activities to improve agency productivity, efficiency, and effectiveness • Ensure DoD compliance with and prompt, efficient, and effective implementation of the information policies and IRM responsibilities established under this subchapter • With respect to general IRM:

Authoritative Source	Mandates
	1) Manage resources to reduce information collection burdens on the public; increase program efficiency and effectiveness; and improve the integrity, quality, and utility of information 2) Maintain a strategic IRM plan 3) Develop and maintain ongoing processes supporting IRM 4) Maintain a current and complete inventory of the agency's information resources 5) Conduct formal training programs to educate agency program and management officials about IRM
Federal Information Security Modernization Act (FISMA) (Title 44 U.S.C., Chapter 35, Subchapter II)	• CIO responsible to ensure agency compliance including: 1) Designate Senior Agency Information Security Officer 2) Develop and maintain Agency-wide Information Security Program 3) Develop and maintain information security policies, procedures, and control techniques 4) Train and oversee personnel with significant information security responsibilities 5) Assist senior officials concerning their information security responsibilities
Federal IT Acquisition Reform Act (FITARA) P.L. 113-291 §§ 831-837	• The Department of Defense is subject to only certain portions of the Federal IT Acquisition Reform Act, including: • Provide recommendations to the Secretary of Defense on DoD IT investments • Certify that IT investments are adequately implementing incremental development • In support of enhanced transparency and improved risk management in IT investments, continue to report non-MIP, non-NSS (National Security Systems) on OMB's IT Dashboard, and categorize the risk of each of those investments • Use the DoD acquisition process and Title 10 to address major IT programs that are rated moderately-high or high risk for more than one year • Conduct annual portfolio review of DoD business (non-NSS) systems • Submit annual reports regarding data center consolidation, including data center inventory, performance metrics, consolidation timeline, and progress (including cost savings) • Manage strategic sourcing • Work with GSA to continue to provide the capability for enterprise software procurement
Department of Defense Directive (DoDD) 5144.02 "DoD Chief Information Officer (DoD CIO)" November 21, 2014; Incorporating Change 1, September 19, 2017	Defined DoD CIO responsibilities: • Develops DoD strategy and policy on the operation and protection of all DoD IT and information systems, including development and promulgation of enterprise-wide architecture requirements and technical standards, and enforcement, operation, and maintenance of systems, interoperability, collaboration, and interface between DoD and non-DoD systems. • Serves as the Agency Chief Information Officer for the DoD with the responsibilities, duties, and qualifications, pursuant to section 11315 of Title 40, U.S.C., and the additional responsibilities, pursuant to section 2223 of Title 10, U.S.C. • Serves as the CIO for DoD with the responsibilities, pursuant to section 3506 of Title 44, U.S.C., related to Federal information policy.

Authoritative Source	Mandates
	• Consistent with section 932 of Public Law 113-66 (FY2014 NDAA), as implemented by Secretary of Defense memorandum (Guidance Regarding Cyberspace Roles, Responsibilities, Functions and Governance within the Department of Defense," June 9, 2014) and Deputy Secretary of Defense memorandum ("Designation of the DoD Principal Cyber Advisor," July 17, 2014), directs, manages, and provides policy guidance and oversight of the DoD cybersecurity program, which includes responsibility for the Defense Information Assurance Program, pursuant to section 2224 of Title 10, U.S.C., and information security, pursuant to section 3544 of Title 44, U.S.C. In the performance of these duties, the DoD CIO, in consultation and coordination with the Under Secretary of Defense for Intelligence, will provide policy guidance to the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), regarding network operations and cybersecurity matters. • Ensures compliance with the requirements of National Security Directive 42 ("National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990) and collaborates with the DIRNSA/CHCSS on the performance of DIRNSA/CHCSS duties, pursuant to National Security Directive 42 and Executive Order 12333 ("United States Intelligence Activities," as amended), as the National Manager for National Security Telecommunications and Information Systems Security. • Consistent with section 171(a) of Title 10, U.S.C. supports the Council on Oversight of the National Leadership Command, Control, and Communications System by providing policy guidance and oversight for the DoD information enterprise that supports DoD C2. This includes the communications, information sharing capabilities, and National Leadership Command Capabilities integrating national, strategic, operational, and tactical C2 and communications systems and programs, including support to the White House Military Office. The DoD CIO develops and oversees contingency and crisis response communications policies and planning for stabilization and reconstruction operations carried out by the DoD with emphasis given to those executed in concert with the U.S. Government interagency process, including DoD interaction with foreign nations and nongovernmental organizations. • Provides guidance and oversight for DoD network operations, including the standards for day-to-day defense and protection of DoD information networks; DoD IT support to military and joint missions; and resilience and reliability of information and communication networks. • Provides policy, oversight, and guidance for matters related to PNT. • Provides policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum and serves as the DoD lead for the management and use of the electromagnetic spectrum; and for electromagnetic environmental effects within DoD, nationally and internationally. The DoD CIO serves as the DoD lead for coordination, approval, and representation of DoD positions on all spectrum matters within the U.S. Government as well as in regional, national, and international spectrum management forums and organizations. • Provides guidance and oversight for the content of those portions of the defense business enterprise architecture that support information

Authoritative Source	Mandates
	technology infrastructure or cybersecurity activities, pursuant to section 2222 of Title 10, U.S.C. • Directs, manages, and provides policy guidance and oversight of the DoD Records Management Program, pursuant to chapters 31 and 33 of Title 44, U.S.C. • Provides guidance and oversight with regard to the recruiting, retention, training, and professional development of the DoD IT and cybersecurity workforce, pursuant to section 11315 of Title 40, U.S.C., and section 3544 of Title 44, U.S.C. The DoD CIO will assess the requirements for agency personnel regarding IRM knowledge and skill and conduct formal training programs to educate agency program and management officials about IRM. • Establishes, maintains, and chairs the DoD CIO Executive Board as the single senior governance forum for DoD IT. The DoD CIO Executive Board provides advice and information to the DoD CIO on the full range of statutory and regulatory matters related to information and DoD IT. • Provides advice on issues related to all assigned responsibilities and functions to: 1) The Defense Business Systems Management Committee and the Defense Business Council, as a co-chair. 2) The Defense Acquisition Board, as a member. 3) The Joint Requirements Oversight Council and Joint Capabilities Integration and Development System process, as an advisor, when appropriate. 4) The Defense Space Council, as a member. 5) The North Atlantic Treaty Organization Command, Control, and Communications Board, as the DoD representative. 6) The Cyber Investment Management Board, as a member. 7) The Council on the Oversight of the National Leadership Command, Control, and Communications System (NLC3S), as a member. • Serves as the chair of the Committee on National Security Systems, pursuant to National Security Directive 42 ("National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990) and Executive Order 13231 ("Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended), and the co-chair of the National Security and Emergency Preparedness Communications Executive Committee, pursuant to Executive Order 13618 ("Assignment of National Security and Emergency Preparedness Communications Functions," July 6, 2012). • Serves on boards, committees, and other groups pertaining to DoD CIO functional areas, and represents the Secretary and Deputy Secretary of Defense on DoD CIO matters outside DoD. • Participates in those planning, programming, budgeting, and execution activities that relate to assigned areas of responsibility. • Reviews assigned functions and responsibilities periodically to ensure that DoD Executive Agent responsibilities resident under the cognizance of the DoD CIO are in conformance with DoDD 5101.1 ("DoD Executive Agent," September 3, 2002, as amended). • Ensures that DoD CIO policies and programs are designed and managed to improve performance standards, economy, and efficiency,

Authoritative Source	Mandates
	and that the Defense Information Systems Agency is attentive to the requirements of its organizational customers, both internal and external to the DoD. • Performs such other duties as the Secretary or Deputy Secretary of Defense may prescribe.
OMB Circular A-130	• The Secretary appoints a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. Military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things: (a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans; (b) Advise the agency head on information resource implications of strategic planning decisions; (c) Advise the agency head on the design, development, and implementation of information resources. (i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project; (ii) Advise the agency head on budgetary implications of information resource decisions; and (d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources; • The Chief Information Officer monitors agency compliance with the policies, procedures, and guidance in Circular A-130. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with the Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1st of each year.

Authorities with Respect to Workforce Management

The DoD Chief Information Officer has cyberspace workforce management responsibilities identified in the Clinger-Cohen Act (1996) and the Paperwork Reduction Act (1995) (codified in 40 USC 11315 and 44 USC 3501 et seq, respectively) regarding hiring, training, professional development and overall IT human capital management. Additionally, the CIO has skill-specific training responsibilities regarding information security (now known as cybersecurity) personnel identified in the Federal Information Security Modernization Act (44 USC 3544).

Consistent with these laws, DoD Directive 5144.02 gives the DoD CIO authority to provide guidance and oversight with regard to the recruiting, retention, training, and professional

development of the IT and cybersecurity categories within the DoD cyber workforce. Accordingly, the DoD CIO will assess the requirements for Department personnel regarding IRM knowledge and skill and conduct formal training programs to educate DoD program and management officials about IRM.