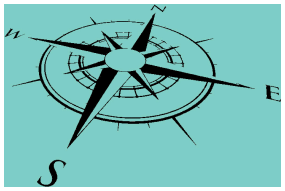
DoD Digital Modernization Strategy

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. 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

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.

Contents



DoD Chief Information Officer (DODCIO)

Description:

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.

Stakeholder(s):

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

Vision

Accelerated transition to foundational enterprise capabilities and services

Mission

To enable Department-wide IT modernization

Values

Modernization: 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. Benefits of this shift will include:

Speed: Increased speed and reduced duplication of effort – increasing IT return on investment (ROI)

Non-Duplication

ROI

Standardization: Consistent, standardized enterprise IT architectures – supporting faster fielding of new capabilities, interoperability, usability, and improved cybersecurity risk exposure

Transparency: Increased budget transparency for DoD IT expenditures

Convergence: Convergence of Component network infrastructure - reducing complexity and cost

Efficiency: Eliminates fielding of unnecessary capabilities and services - reducing program overhead

Cost Effectiveness: Enterprise acquisition/licensing discounts - reducing infrastructure and application licenses

Agility: 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.

Resilience

Simplicity

Innovation: 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.

Security

1. Innovation

Innovate for Competitive Advantage

Stakeholder(s)

Joint Artificial Intelligence Center (JAIC) :
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.

DoD Information Network (DODIN) :
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).

Defense Information Systems Network (DISN) :
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

Joint Force :
Increased availability and use of secure, mobile, wireless platforms across the Department will increase Joint Force maneuver, accuracy, and information advantage.

Healthcare Functions :
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.

Logistics Functions

Warfighting Support Functions

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.

1.1. JAIC

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

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.

Stakeholder(s):

Joint Artificial Intelligence Center (JAIC)

Performance Indicators

Strategy Element 1.1.1 Operations

Description	Type	Status	Start Date	End Date
Stand Up the JAIC and Initiate Operations	Target	Initiation		
	Actual			

Strategy Element 1.1.2 Partnerships

Description	Type	Status	Start Date	End Date
Establish Partnerships with Industry, Academia, and Partner Nations to Ensure State-of-the-Art AI Capabilities	Target	Initiation		
	Actual			

Strategy Element 1.1.3 Infrastructure Technology Stack

Description	Type	Status	Start Date	End Date
Develop and Sustain the Enterprise Infrastructure Technology Stack that Enables AI Capability Deployment at Speed and Scale (JAIC Common Foundation)	Target	Development		
	Target	Sustainment		
	Actual			

Strategy Element 1.1.4 AI Leadership

Description	Type	Status	Start Date	End Date
Lead DoD in AI Planning, Policy, Oversight, Ethics, and Safety	Target	Leadership		
	Actual			

Strategy Element 1.1.5 AI Capabilities

Description	Type	Status	Start Date	End Date
Deliver AI-Enabled Capabilities to Address Key Missions (National Mission Initiatives, Component Mission Initiatives, and Smart Automation Initiatives)	Target	Delivery		
	Actual			

Strategy Element 1.1.6 AI Assurance/Certification

Description	Type	Status	Start Date	End Date
Assure /Certify the AI Algorithms, Data, and Models Developed for JAIC Implementations	Target	Assurance		
	Target	Certification		
	Actual			

1.2. Commercial Innovation

Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation

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.

Stakeholder(s):

DoD CIO :
DoD CIO will collaborate with DoD Components (e.g., OUSD(R&E), MILDEPS, Combatant Commands) to support achievement of this objective.

OUSD(R&E)

MILDEPS

Combatant Commands

Performance Indicators

Strategy Element 1.2.1 Cloud

Description	Type	Delivery	Start Date	End Date
Deliver a General-Purpose Enterprise Cloud for Compute and Store Capabilities (i.e., Joint Enterprise Defense Infrastructure (JEDI))	Target	Delivered		
	Actual			

Strategy Element 1.2.2 Capabilities

Description	Type	Identification	Start Date	End Date
Identify Common Niche Capabilities to Inform the Creation of Fit for Purpose (F2P) Cloud Environments	Target	Identification		
	Actual			

Strategy Element 1.2.3 Environment

Description	Type	Provisioning	Start Date	End Date
Provide a DoD On Premise Cloud Environment	Target	Provided		
	Actual			

Strategy Element 1.2.4 Office

Description	Type	Establishment	Start Date	End Date
Establish an Enterprise Cloud Office to Enable Rapid Acquisition, Deployment, and Migration to Cloud Capabilities	Target	Established		
	Actual			

Strategy Element 1.2.5 Portfolio

Description	Type	Management	Start Date	End Date
Manage the DoD Portfolio of Cloud Capabilities	Target	Managed		
	Actual			

Strategy Element 1.2.6 Policy & Guidance

Description	Type	Development	Start Date	End Date
Develop Policy and Guidance to Modernize Application Development (e.g., Lean-Agile Practices)	Target	Developed		
	Actual			

Strategy Element 1.2.7 DevSecOps Environment

Description	Type	Development & Deployment	Start Date	End Date
Develop and Deploy a DevSecOps Environment that Enables Application Development and Accreditation at Speed and Scale Integrated with Defensive Cyberspace Operations	Target	Developed		
	Target	Deployed		
	Actual			

Strategy Element 1.2.8 Policy & Guidance

Description	Type	Development	Start Date	End Date
Develop Policy and Guidance on the Effective Application of DevSecOps Principles	Target	Developed		
	Actual			

Strategy Element 1.2.9 Resilient Operation

Description	Type	Enablement	Start Date	End Date
Enable Resilient Operation of DoD Functions on Commercial Cloud Infrastructure	Target	Enabled		
	Actual			

1.3. C4

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

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.

Stakeholder(s):

C4 Systems

MILDEPS

OUSD(R&E)

Combatant Commands

Performance Indicators

Strategy Element 1.3.1 Strategies, Roadmaps, Plans, & Architectures

Description	Type	Production	Start Date	End Date
Strategies - Produce C4 Strategies, Roadmaps, Plans, and Architectures Roadmaps	Target	Produced		
	Target	Produced		
Plans	Target	Produced		
Architectures	Target	Produced		
	Actual			

Strategy Element 1.3.2 Policies

Description	Type	Status	Start Date	End Date
Update and Publish Required Tactical Communications Policies	Target	Updated		
	Target	Published		
	Actual			

Strategy Element 1.3.3 C4 Capabilities

Description	Type	Synchronization	Start Date	End Date
Synchronize Enterprise C4 Capabilities through Effective Governance	Target	Synchronized		
	Actual			

Strategy Element 1.3.4 Radios & Waveform Capabilities

Description	Type	Modernization	Start Date	End Date
Modernize Tactical Radios and DoD Tactical Waveform Capabilities	Target	Modernized		
	Actual			

Strategy Element 1.3.5 Public Safety Communications Enterprise Architecture

Description	Type	Status	Start Date	End Date
Develop and Maintain the Enterprise Architecture for DoD Public Safety Communications	Target	Developed		
	Target	Maintained		
	Actual			

Strategy Element 1.3.6 EMWN

Description	Type	Implementation	Start Date	End Date
Implement DoD Global Enterprise Mass Warning & Notification (EMWN) Capabilities	Target	Implemented		
	Actual			

Strategy Element 1.3.7 GCCS-J

Description	Type	Modernization	Start Date	End Date
Modernize the Global Command and Control System - Joint (GCCS-J)	Target	Modernized		
	Actual			

Strategy Element 1.3.8 Satellite Communications

Description	Type	Modernization	Start Date	End Date
Modernize DoD Satellite Communications Management and Control	Target	Modernized		
	Actual			

Strategy Element 1.3.9 PSCS & WCS

Description	Type	Execution	Start Date	End Date
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	Target	Executed		
	Actual			

Strategy Element 1.3.10 Management & Control

Description	Type	Formalization & Implementation	Start Date	End Date
Formalize and Implement the Enterprise SATCOM Management and Control Reference Architecture	Target	Formalized		
	Target	Implemented		
	Actual			

1.4. Data

Treat Data as a Strategic Asset

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.

Performance Indicators

Strategy Element 1.4.1 Data Tags

Description	Type	Definition	Start Date	End Date
Define a Minimum Essential Set of Enterprise Data Tags that Enable the Tenets of DoDI 8320.07	Target			
	Actual			

Strategy Element 1.4.2 Infrastructure

Description	Type	Status	Start Date	End Date
Invest In and Maintain the Infrastructure Required to Make DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable	Target	Visibility		
	Target	Accessibility		
	Target	Understandability		
	Target	Trustworthiness		
	Target	Interoperability		
	Actual			

1.5. Collaboration, Partnerships & Interoperability

Strengthen Collaboration, International Partnerships, and Allied Interoperability

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.

Stakeholder(s):

North Atlantic Treaty Organization (NATO)

Allies

International Partners

Performance Indicators

Strategy Element 1.5.1 MILSATCOM

Description	Type	Development	Start Date	End Date
Develop Military Satellite Communications (MILSATCOM) Services, Infrastructure, and Standards with International Partners	Target	Developed		
	Actual			

Strategy Element 1.5.2 Processes & Method

Description	Type	Improvement & Standardization	Start Date	End Date
Improve Tactical Communications Waveform Export Processes and Develop a Standardized Method to ~~Address CCMD Connection Requests~~ between US and Allied/Coalition Systems	Target	Improvement		
	Target	Standardization		
	Actual			

Strategy Element 1.5.3 Communications Planning

Description	Type	Advancement	Start Date	End Date
Advance Civil Emergency Communications Planning with DoD, NATO, Allies, and Other International Partners	Target	Advanced		
	Actual			

Strategy Element 1.5.4 ICAM

Description	Type	Assurance	Start Date	End Date
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	Target	Assured		
	Actual			

Strategy Element 1.5.5 Cryptographic Products

Description	Type	Flexibility & Robustness	Start Date	End Date
Develop Flexible and Robust Secure Cryptographic Products for Seamless Secure Foreign Partner Interoperability	Target	Flexible		
	Target	Robust		
	Actual			

Strategy Element 1.5.6 Processes & Decision-Making

Description	Type	Streamlining	Start Date	End Date
Streamline Release Processes and Decision-making to Advance U.S. Security Cooperation	Target	Streamlined		
	Actual			

Strategy Element 1.5.7 Requirements & Processes

Description	Type	Implementation	Start Date	End Date
Implement the MPE Requirements and Portfolio Management Processes	Target	Implemented		
	Actual			

Strategy Element 1.5.8 Information Sharing

Description	Type	Rationalization	Start Date	End Date
Rationalize Coalition C2 and Intelligence Information Sharing Capabilities	Target	Rationalized		
	Actual			

Strategy Element 1.5.9 Capability & Services

Description	Type	Delivery	Start Date	End Date
Deliver the DoD MPE Capability and Services	Target	Delivered		
	Actual			

1.6. Connectivity

Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity

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.

Performance Indicators

Strategy Element 1.6.1 Conferencing

Description	Type	Capability	Start Date	End Date
Evaluate Current Conferencing Capability and If Required, Develop a Methodology that Improves Secure, Survivable Conferencing	Target	Evaluated		
	Target	Improved		
	Actual			

Strategy Element 1.6.2 Collection & Display

Description	Type	Enhancement	Start Date	End Date
Collection	Target	Enhanced		
Display	Target	Enhanced		
	Actual			

Enhance Current Data Collection and Display Processes to Provide Senior Leadership-Quality Decision-Making Information

Strategy Element 1.6.3 Process

Description	Type	Delivery	Start Date	End Date
Develop a Process that Delivers a Classified, Secure, and Mobile Solution that Meets Senior Leadership Requirements	Target	Delivered		
	Actual			

Strategy Element 1.6.4 Security

Description	Type	Enhancement	Start Date	End Date
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	Target	Enhanced		
	Actual			

1.7. PNT

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

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.

Performance Indicators

Strategy Element1.7.1 Approaches

Description	Type	Implementation	Start Date	End Date
Pursue DoD Implementation of a Modular Open Systems Approaches and Collaborative Modeling and Simulation (M&S) Approach for PNT Capabilities	Target	Implemented		
	Actual			

Strategy Element 1.7.2 Roadmap

Description	Type	Development & Publication	Start Date	End Date
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))	Target	Development		
	Target	Publication		
	Actual			

Strategy Element 1.7.3 MGUE

Description	Type	Tracking & Assistance	Start Date	End Date
Track and Assist in Modifying Plans for Military GPS User Equipment (MGUE) Development and Production	Target	Tracked		
	Target	Assisted		
	Actual			

Strategy Element 1.7.4 Capabilities

Description	Type	Fielding	Start Date	End Date
Field Modernized PNT Capabilities with the Air Force and Our International Allies	Target	Fielded		
	Actual			

Strategy Element 1.7.5 Partnerships

Description	Type	Development	Start Date	End Date
Develop Navigation Warfare (NAVWAR) Partnerships with Closely Allied Nations	Target	Developed		
	Actual			

Strategy Element 1.7.6 Capabilities

Description	Type	Evaluation & Demonstration	Start Date	End Date
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))	Target	Evaluated		
	Target	Demonstrated		
	Actual			

Strategy Element 1.7.7 Oversight

Description	Type	Advantage	Start Date	End Date
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	Target			
	Actual			

Strategy Element 1.7.8 Issuances

Description	Type	Development & Compliance	Start Date	End Date
Develop New (and Maintain Existing) DoD Issuances to Facilitate Policy Implementation and Ensure DoD Component Compliance for the DoD PNT Enterprise	Target	Developed		
	Target	Compliance		
	Actual			

Strategy Element 1.7.9 Data Collection

Description	Type	Institutionalization	Start Date	End Date
Continue to Institutionalize the PNT Data Repository Data Collection Process	Target	Institutionalized		
	Actual			

1.8. DISN

Modernize Defense Information Systems Network (DISN) Transport Infrastructure

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.

Performance Indicators

Strategy Element 1.8.1 Optical Transport

Description	Type	Upgrading	Start Date	End Date
Upgrade Optical Transport	Target	Upgraded		
	Actual			

Strategy Element 1.8.2 Mid-Point Security

Description	Type	Implementation	Start Date	End Date
Enhance Mid-Point Security by Implementing JRSS and Joint Management System (JMS)	Target	Implemented		
	Actual			

Strategy Element 1.8.3 MPLS

Description	Type	Build Out	Start Date	End Date
Build Out Multi-Protocol Label Switching (MPLS) Router Network with Quality of Service and Performance Monitoring	Target	Built Out		
	Actual			

Strategy Element 1.8.4 SDN

Description	Type	Implementation	Start Date	End Date
Implement Software Defined Networking (SDN)	Target	Implemented		
	Actual			

Strategy Element 1.8.5 ATM

Description	Type	Elimination	Start Date	End Date
Eliminate Asynchronous Transfer Mode (ATM) and Low Speed Time Division Multiplexed (TDM) Circuits	Target	Eliminated		
	Actual			

Strategy Element 1.8.6 IPv6

Description	Type	Implementation	Start Date	End Date
Implement Internet Protocol version 6 (IPv6)	Target	Implemented		
	Actual			

1.9. Networks & Services

Modernize and Optimize DoD Component Networks and Services

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.

Performance Indicators

Strategy Element 1.9.1 Networks

Description	Type	Consolidation & Optimization	Start Date	End Date
Consolidate and Optimize Fourth Estate Networks	Target	Consolidated		
	Target	Optimized		
	Actual			

Strategy Element 1.9.2 Service Desks

Description	Type	Consolidation	Start Date	End Date	Number
Consolidate the Number of Fourth Estate Service Desks into a Single Service Support Environment	Target	Consolidated			1
	Actual				

Strategy Element 1.9.3 NOCs/SOCs

Description	Type	Consolidation & Optimization	Start Date	End Date
Consolidate and Optimize the Fourth Estate Network Operation Centers/ Security Operations Centers (NOCs/ SOCs)	Target	Consolidated		
	Target	Optimized		
	Actual			

Strategy Element 1.9.4 Best Practices

Description	Type	Establishment	Start Date	End Date
Establish Best Practices for Component Use of Commercial Service Providers in Their Optimization and Modernization Efforts	Target	Established		
	Actual			

1.10. AISR DT

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

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.

Performance Indicators

Strategy Element 1.10.1 Capabilities

Description	Type	Establishment	Start Date	End Date
Establish Capabilities to Support Ingest, Accumulation, and Global Delivery of AISR Data from Multiple Platforms/Sources	Target	Established		
	Actual			

Strategy Element 1.10.2 Tactical Relays

Description	Type	Construction	Start Date	End Date
Build Tactical Relays for Sensor Platform Connectivity to Local Users and the DISN	Target	Constructed		
	Actual			

Strategy Element 1.10.3 BLOS

Description	Type	Connectivity	Start Date	End Date
Provide Global Satellite Gateways for Direct Beyond Line of Sight (BLOS) Connectivity Between AISR Platforms and the DISN	Target	Provided		
	Actual			

Strategy Element 1.10.4 Network Operations

Description	Type	Establishment	Start Date	End Date
Establish Network Operations to Support End-to-End Situational Awareness and Proactive Network Management	Target	Established		
	Actual			

Strategy Element 1.10.5 Transport Capabilities

Description	Type	Direction	Start Date	End Date
Provide Direction for Future Platform Transport Capabilities	Target	Provided		
	Actual			

1.11. Information Sharing

Improve Information Sharing to Mobile Users

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

Stakeholder(s):

Mobile Users

Performance Indicators

Strategy Element 1.11.1 Purchasing

Description	Type	Streamlining	Start Date	End Date
Streamline the Purchasing of Mobile Devices and Services across the DoD Enterprise	Target			
	Actual			

Strategy Element 1.11.2 Portfolio Management

Description	Type	Efficiency & Effectiveness	Start Date	End Date
Improve Mobile Policies, Processes, and Procedures to Ensure Efficient and Effective Portfolio Management	Target			
	Actual			

Strategy Element 1.11.3 Credentials

Description	Type	Usage	Start Date	End Date
Expand Use of Derived Credentials for Mobile	Target	Expansion		
	Actual			

Strategy Element 1.11.4 Applications

Description	Type	Development	Start Date	End Date
Develop Applications of Tactical Mobility	Target			
	Actual			

Strategy Element 1.11.5 Device Security

Description	Type	Status	Start Date	End Date
Establish a Mobile Device Security Architecture and Risk Management Approach in Collaboration with Five Eyes (FVEY) Mission Partners	Target	Security Architecture		
	Target	Risk Management Approach		
	Actual			

Strategy Element 1.11.6 FirstNet

Description	Type	Status	Start Date	End Date
	Target	Way-Ahead		
	Target	Policy		
Establish DoD Way-Ahead, Policy, and Plans for Use of the National First Responder Network (FirstNet) in Support of DoD Public Safety Communications	Target	Plans		
	Actual			

Strategy Element 1.11.7 5G

Description	Type	Status	Start Date	End Date
DoD Will Be an Early Adopter of 5G and Develop Applications to Leverage 5G Advanced Capabilities	Target	Adoption		
	Target	Application Development		
	Actual			

1.12. EMSO

Evolve the DoD to Agile Electromagnetic Spectrum Operations (EMSO)

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.

Performance Indicators

Strategy Element 1.12.1 Data Sharing

Description	Type	Capability	Start Date	End Date
Establish an EMSO Multi-Tiered Architecture Capable of Sharing EMS Data Between All Services and Agencies at All Classification Levels	Target			
	Actual			

Strategy Element 1.12.2 Network Infrastructure

Description	Type	Status	Start Date	End Date
Establish a Resilient, Secure, and Adaptive EMSO IT Network Infrastructure	Target	Resiliency		
	Target	Security		
	Target	Adapability		
	Actual			

1.13. Standards

Drive Standards into DoD IT Systems

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.

Performance Indicators

Strategy Element 1.13.1 Gaps

Description	Type	Status	Start Date	End Date
Assess and Identify Gaps in Policy for IT, Networking, Data, and Cybersecurity Standards	Target	Identification		
	Target	Resolution		
	Actual			

Strategy Element 1.13.2 Strategy

Description	Type	Status	Start Date	End Date
Develop Strategy for Addressing Gaps in Processes, Governance, Policy, and Standards	Target	Development		
	Actual			

Strategy Element 1.13.3 Implementation

Description	Type	Status	Start Date	End Date
Implement Revised Processes, Governance, Policy, and Standards	Target	Implemented		
	Actual			

Strategy Element 1.13.4 Compliance

Description	Type	Enforcement	Start Date	End Date
Monitor and Enforce Compliance with Revised Processes, Governance, Policy, and Standards	Target	Compliance		
	Actual			

2. Efficiency & Capabilities

Optimize for Efficiencies and Improved Capability

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.

2.1. Enterprise-Wide Model

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

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.

Performance Indicators

Strategy Element 2.1.1 Operations Centers

Description	Type	Enablement	Start Date	End Date
Enable Global and Regional Operations Centers	Target	Enabled		
	Actual			

Strategy Element 2.1.2 Management Network

Description	Type	Establishment & Implementation	Start Date	End Date
Establish and Implement the JIE Management Network for JRSS	Target	Established		
	Target	Implemented		
	Actual			

Strategy Element 2.1.3 ITSM Solutions

Description	Type	Convergence	Start Date	End Date
Converge DODIN IT Service Management (ITSM) Solutions	Target	Converged		
	Actual			

Strategy Element 2.1.4 COP Solutions

Description	Type	Convergence	Start Date	End Date
Converge DODIN Operation Common Operation Picture (COP) Solutions	Target	Converged		
	Actual			

2.2. Data Centers

Optimize DoD Data Centers

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.

Stakeholder(s):

DoD Data Centers

Performance Indicators

Strategy Element 2.2.1 Applications & Systems

Description	Type	Migration	Start Date	End Date
Migrate DoD Applications and Systems that Cannot be Hosted in Commercial Cloud Environments to Enterprise Data Centers	Target	Migrated		
	Actual			

Strategy Element 2.2.2 Data Centers

Description	Type	Optimization	Start Date	End Date
Optimize Select Data Centers for Performance First, Then Cost	Target	Optimized		
	Actual			

Strategy Element 2.2.3 Installation Processing Nodes

Description	Type	Re-Designation	Start Date	End Date
Re-designate Installation Processing Nodes in Accordance with the Department's Current Data Center Optimization Approach	Target	Re-Designated		
	Actual			

Strategy Element 2.2.4 Data Center Inventory

Description	Type	Management	Start Date	End Date
Manage the DoD Data Center Inventory for Mission Need	Target	Managed		
	Actual			

2.3. Productivity & Collaboration

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

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

Performance Indicators

Strategy Element 2.3.1 DEOS

Description	Type	Status	Start Date	End Date
Designate DEOS as a DoD Enterprise Service with all DoD Components Required to Adopt	Target	Designation		
	Target	Adoption		
	Actual			

Strategy Element 2.3.2 Pilots

Description	Type	Monitoring & Assessment	Start Date	End Date
Monitor and Assess All Pilots for Implementation Pitfalls and Challenges, including D-DIL	Target	Monitored		
	Target	Assessed		
Roll All Lessons Learned from Early Cloud Adopters into DEOS	Target	Implemented		
	Actual			

Strategy Element 2.3.3 DEOS

Description	Type	Fielding & Migration	Start Date	End Date
Field DEOS (including in D-DIL Environments) and Complete Migration of All DoD Users	Target	Fielded		
	Target	Completed		
	Actual			

2.4. Voice & Video

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

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.

Performance Indicators

Strategy Element 2.4.1 Voice & Video

Description	Type	Definition & Deployment	Start Date	End Date
Define and Deploy an Optimized Enterprise Voice and Video Solution across the Department (e.g., ECAPS Capability Sets 2 and 3)	Target	Defined		
	Target	Deployed		
	Actual			

Strategy Element 2.4.2 C2 Voice Solution

Description	Type	Definition & Deployment	Start Date	End Date
Define and Deploy an Optimized DoD C2 Voice Solution	Target	Defined		
	Target	Deployed		
	Actual			

Strategy Element 2.4.3 Analog Phone Switch

Description	Type	Elimination	Start Date	End Date
Eliminate DoD's Legacy Analog Phone Switch Infrastructure	Target	Eliminated		
	Actual			

Strategy Element 2.4.4 NG911

Description	Type	Status	Start Date	End Date
Establish DoD Way-Ahead, Policy, and Plans for Employment of Next Generation 9-1-1 (NG911)	Target	Established		
Policy	Target	Established		
Plans	Target	Established		
	Actual			

2.5. Category Management

Improve IT Category Management

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

Performance Indicators

Strategy Element 2.5.1 ELAs

Description	Type	Status	Start Date	End Date
Continue to Establish ELAs for IT Software, Hardware, Services, and Telecommunications	Target	Established		
	Actual			

Strategy Element 2.5.2 ELAs

Description	Type	Expansion	Start Date	End Date
Expand ELAs to Address Other IT Categories (e.g., IT Security) Based on OMB Guidance	Target	Expanded		
	Actual			

Strategy Element 2.5.3 Category Management Policy

Description	Type	Status	Start Date	End Date
Establish DoD Category Management Policy	Target	Established		
	Actual			

Strategy Element 2.5.4 Asset Management

Description	Type	Implementation	Start Date	End Date
Implement DoD IT Asset Management	Target	Implemented		
	Actual			

2.6. Technology Deployment

Improve Rapid Technology Deployment Processes

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.

Performance Indicators

Strategy Element 2.6.1 Approval Process

Description	Type	Streamlining	Start Date	End Date
Streamline the Technology Approval Process	Target	Streamlined		
	Actual			

Strategy Element 2.6.2 OTAs

Description	Type	Leveraging	Start Date	End Date
Leverage the Power and Agility of Other Transactional Agreements (OTAs)	Target	Leveraged		
	Actual			

2.7. Financial Management

Strengthen IT Financial Management Decision Making and Accountability

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.

Performance Indicators

Strategy Element 2.7.1 Audit Readiness

Description	Type	Support	Start Date	End Date
Support Audit Readiness for Financial and Mixed Systems that Impact Financial Reporting	Target	Supported		
	Actual			

Strategy Element 2.7.2 Accountability & Auditability

Description	Type	Improvement	Start Date	End Date
Improve Accountability and Auditability for Internal Use Software Investments	Target	Improved		
	Actual			

Strategy Element 2.7.3 Oversight & Certification

Description	Type	Status	Start Date	End Date
Implement FY2018 NDAA Requirements Regarding Oversight and Certification of Component IT Budgets	Target	Implemented		
	Actual			

3. Cybersecurity

Evolve Cybersecurity for an Agile and Resilient Defense Posture

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 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.

3.1. Architecture

Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience

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.

Performance Indicators

Strategy Element 3.1.1 Security & Monitoring

Description	Type	Improvement	Start Date	End Date
Improve Endpoint Security and Continuous Monitoring	Target	Improved		
	Actual			

Strategy Element 3.1.2 Perimeter Protection

Description	Type	Enhancement	Start Date	End Date
Enhance Enterprise Perimeter Protection Capabilities	Target	Enhanced		
	Actual			

Strategy Element 3.1.3 Comply-to-Connect

Description	Type	Status	Start Date	End Date
Establish Enterprise Comply-to-Connect Capability	Target	Established		
	Actual			

Strategy Element 3.1.4 Insider Threat Detection

Description	Type	Status	Start Date	End Date
Deploy Insider Threat Detection Capabilities	Target	Deployed		
	Actual			

Strategy Element 3.1.5 Data Center Security

Description	Type	Strengthening	Start Date	End Date
Strengthen Data Center Security	Target	Strengthened		
	Actual			

Strategy Element 3.1.6 SHB

Description	Type	Standardization	Start Date	End Date
Standardize on Windows 10 Secure Host Baseline (SHB)	Target	Standardized		
	Actual			

Strategy Element 3.1.7 Patch Management

Description	Type	Automation	Start Date	End Date
Implement Automated Patch Management	Target	Automated		
	Actual			

Strategy Element 3.1.8 Situational Awareness

Description	Type	Enhancement	Start Date	End Date
Enhance Cybersecurity Situational Awareness through Big Data Analytics	Target	Enhanced		
	Actual			

Strategy Element 3.1.9 Cryptography

Description	Type	Modernization	Start Date	End Date
Modernize the Cryptographic Inventory and Supporting Infrastructure	Target	Modernized		
	Actual			

3.2. ICAM

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

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/nonperson 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.

Performance Indicators

Strategy Element 3.2.1 Public Key

Description	Type	Enablement	Start Date	End Date
Expand Public Key Enablement Capabilities to Support ICAM	Target	Expanded		
	Actual			

Strategy Element 3.2.2 Account Provisioning

Description	Type	Automation	Start Date	End Date
Implement Automated Account Provisioning	Target	Implemented		
	Actual			

Strategy Element 3.2.3 Multi-Factor Authentication

Description	Type	Status	Start Date	End Date
Implement Support for Approved Multi-Factor Authentication Capabilities	Target	Implemented		
	Actual			

Strategy Element 3.2.4 EIAS

Description	Type	Enhancement	Start Date	End Date
Enhance Enterprise Identity Attribute Service (EIAS)	Target	Enhanced		
	Actual			

Strategy Element 3.2.5 Derived Credentials

Description	Type	Usage	Start Date	End Date
Expand the Use of Derived Credentials	Target	Expanded		
	Actual			

Strategy Element 3.2.6 Identity & Attributes

Description	Type	Data Centricity	Start Date	End Date
Implement a Data Centric Approach to Collect, Verify, Maintain, and Share Identity and Other Attributes	Target	Implemented		
	Actual			

Strategy Element 3.2.7 Authentication

Description	Type	Improvement & Enablement	Start Date	End Date
Common Standards - Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation	Target	Implemented		
	Target	Shared		
Federation	Target	Supported		
	Actual			

Strategy Element 3.2.8 ICAM

Description	Type	Shared Services	Start Date	End Date
Deploy Shared Services Promoting the Implementation of Enterprise ICAM	Target	Deployed		
	Actual			

Strategy Element 3.2.9 Monitoring & Logging

Description	Type	Enablement	Start Date	End Date
Enable Consistent Monitoring and Logging to Support Identity Analytics for Detecting Insider Threats and External Attacks	Target	Enabled		
	Actual			

Strategy Element 3.2.10 Governance Structure

Description	Type	Enhancement	Start Date	End Date
Enhance the Governance Structure Promoting the Development and Adoption of Enterprise ICAM Solutions	Target	Enhanced		
	Actual			

Strategy Element 3.2.11 Policies & Standards

Description	Type	Creation	Start Date	End Date
Create DoD Policies and Standards Clearly Defining Requirements for Identification, Credentialing, Authentication, and Authorization Lifecycle Management	Target	Created		
	Actual			

3.3. Unclassified Networks & Systems

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

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.

Performance Indicators

Strategy Element 3.3.1 Procedures

Description	Type	Development	Start Date	End Date
Support Development of Consistent Procedures to Assess Contractor Compliance with Cybersecurity Requirements	Target	Developed		
	Actual			

Strategy Element 3.3.2 NIST SP 800-171

Description	Type	Updating	Start Date	End Date
Support Efforts to Update NIST SP 800-171 to Address Advanced Persistent Threats	Target	Updated		
	Actual			

Strategy Element 3.3.3 Participation

Description	Type	Increase	Start Date	End Date
Increase Participation in the DIB Cybersecurity Program	Target	Increased		
	Actual			

Strategy Element 3.3.4 Information Sharing

Description	Type	Expansion	Start Date	End Date
Expand Cybersecurity Threat Information Sharing to Non-Cleared Defense Contractors	Target	Expanded		
	Actual			

Strategy Element 3.3.5 Cybersecurity Pathfinders

Description	Type	Planning & Execution	Start Date	End Date
Plan and Execute DIB Cybersecurity Pathfinders	Target	Planned		
	Target	Executed		
	Actual			

3.4. Risk Management

Reform DoD Cybersecurity Risk Management Policies and Practices

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.

Performance Indicators

Strategy Element 3.4.1 Framework Reform

Description	Type	Advancement	Start Date	End Date
Advance Risk Management Framework Reform to Ensure it is More Efficient and Adaptable	Target	Advanced		
	Actual			

Strategy Element 3.4.2 Cybersecurity Risk

Description	Type	Management	Start Date	End Date
Ensure Cybersecurity Risks are Planned for and Managed Throughout the Acquisition Lifecycle	Target	Managed		
	Actual			

Strategy Element 3.4.3 Supply Chain Risk

Description	Type	Reduction	Start Date	End Date
Enhance Processes to Address Enterprise-Wide Supply Chain Risks	Target	Reduced		
	Actual			

Strategy Element 3.4.4 Portfolio Management

Description	Type	Strengthening	Start Date	End Date
Strengthen the DoD Cybersecurity Portfolio Management Process	Target	Strengthened		
	Actual			

Strategy Element 3.4.5 Assurance

Description	Type	Expansion	Start Date	End Date
Expand the Use of Proven Software and Hardware Assurance Methods	Target	Expanded		
	Actual			

Strategy Element 3.4.6 Cooperation

Description	Type	Robustness	Start Date	End Date
Build and Maintain Robust International Cybersecurity Cooperation Efforts	Target	Increasing		
	Actual			

Strategy Element 3.4.7 Standards

Description	Type	Participation	Start Date	End Date
Increase DoD Participation in Setting Federal Government and International Commercial Cybersecurity Standards	Target	Increased		
	Actual			

4. Digital Workforce

Cultivate Talent for a Ready Digital Workforce

Stakeholder(s)

Digital Workforce

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).

4.1. Cyber Functional Community

Strengthen Cyber Functional Community Management

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

Stakeholder(s):

Cyber Functional Community

Performance Indicators

Strategy Element 4.1.1 Maturity Model

Description	Type	Implementation	Start Date	End Date
Implement the Functional Community Maturity Model for the IT and Cybersecurity Categories of the Cyber Workforce	Target	Implemented		
	Actual			

Strategy Element 4.1.2 Role Gaps

Description	Type	Identification & Targeting	Start Date	End Date
Identify and Target Work Role Gaps of Critical Need for the Cyber (IT and Cybersecurity) Workforce	Target	Identified		
	Target	Targeted		
	Actual			

4.2. Acquisition Workforce

Strengthen the IT Acquisition Workforce

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.

Stakeholder(s):

Acquisition Workforce

Performance Indicators

Strategy Element 4.2.1 Competencies

Description	Type	Strengthening	Start Date	End Date
Strengthen IT Acquisition Workforce Competencies	Target	Strengthened		
	Actual			

Strategy Element 4.2.2 Curriculum & Capabilities

Description	Type	Updating & Maintenance	Start Date	End Date
Update Curriculum Requirements and Maintain Continuous Learning Capabilities	Target	Updated		
	Target	Maintained		
	Actual			

4.3. Cyber Workforce

Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development

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.

Stakeholder(s):

Cyber Workforce

Performance Indicators

Strategy Element 4.3.1 Excepted Service

Description	Type	Expansion	Start Date	End Date
Expand Implementation of Cyber Excepted Service	Target	Expanded		
	Actual			

Strategy Element 4.3.2 Program

Description	Type	Implementation	Start Date	End Date
Implement Cyber Workforce Qualifications Program	Target	Implemented		
	Actual			

Administrative Information

Start Date: 2019-07-12
End Date:

Publication Date: **2019-07-25**
Source: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

Submitter:
Given Name: **Surname:**
Email: **Phone:**