FULCRUM:
THE DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY ADVANCEMENT STRATEGY

A Letter from the Deputy Secretary of Defense

Our ability to operate successfully in the digital age hinges on our ability to leverage the power of information technology. By optimizing the use of innovative products, improving IT user experiences, and enhancing operational effectiveness, we can accelerate the Department's modernization efforts and expand our military's strategic advantage.

That's why I am pleased to share with you *Fulcrum: The Department of Defense (DoD) Information Technology {IT) Advancement Strategy*. Fulcrum provides a roadmap for better aligning our information technology usage to advance Department priorities.

To succeed, today's warfighter requires information technology that is compatible with the complex demands of a dynamic operating environment and modem battlefield. Technology that enables functional, rapid, and secure support. This strategy relies on four distinct lines of effort that recognize this imperative as critical to meeting our national security needs.

At the heart of our approach is a steadfast commitment to user-centricity ensuring that user experiences are intuitive and adaptable. To achieve this objective, this strategy focuses on ensuring our IT systems are fully integrated, our capabilities are best- in-class, our infrastructure is resilient and secure, and our IT management processes are efficient and agile enough to move at the speed and scale needed to support and achieve our operational needs at any given moment.

Finally, we are committed to cultivating a highly-skilled and diverse digital workforce. One that reflects a rich tapestry of perspectives and expertise. Through targeted recruitment efforts, we can attract top-tier talent to drive innovation. And through training and development initiatives, we empower our employees to lead this digital transformation and deliver excellence at every turn.

Together, we will continue to adapt in a dynamic technology landscape while delivering premier IT capabilities to the warfighter and superior value to the American taxpayer. This strategy guides the way.

The Honorable Kathleen H. Hicks
Deputy Secretary of Defense

Strategic Intent

Fulcrum represents the Department's ambitious Information Technology (IT) advancement strategy designed to leverage the power of technology to drive transformative change and serves as a tipping point for catalyzing digital modernization for the warfighter.

To propel the Department forward, we must ensure continued success and relevance in the digital age. Fulcrum will enable achievement of the DoD mission and strategic objectives with unparalleled efficiency and effectiveness. To do so, the Department must:

- Deliver solutions that are innovative, feature-rich, and aligned with user needs.
- Prioritize user experience (UX) by ensuring that **functionality** is intuitive, performant, resilient, and contributes to overall mission success.
- Invest in IT infrastructure that is **agile** and **scalable**, capable of adapting to ever changing business requirements and mission demands.
- Implement measures to maintain optimal performance, even during periods of increased workloads or business expansion.
- Consider long-term **interoperability** and **sustainability** of IT solutions during design and development aiming for solutions that stand the test of time.
- Implement secure by design principles paired with a robust **cybersecurity** management framework that addresses the entire IT landscape, from network infrastructure to applications and data.

The DoD Chief Information Officer's (DoD CIO) mission is to **connect**, **protect**, and **perform**. Fulcrum outlines a vision guided by four lines of effort (LOEs) representing a strategic shift that embraces technology as a mission enabler. The following LOEs drive sustainable growth, enhance operational effectiveness, and deliver superior value to the Warfighter:

- **LOE 1: Provide Joint Warfighting IT capabilities** to expand strategic dominance of U.S. Forces & mission partners.
- **LOE 2: Modernize information networks and compute** to rapidly meet mission and business needs.
- **LOE 3: Optimize IT governance** to gain efficiencies in capability delivery and enable cost savings.
- **LOE 4: Cultivate a premier digital workforce** ready to deploy emerging technology to the warfighter.

Fulcrum features the DoD CIO's IT goals and objectives for Fiscal Years (FYs) 2025-2029 that provide essential support to the priorities in the National Defense Strategy (NDS), and the supporting DoD Strategic Management Plan (SMP). The figure below demonstrates that Fulcrum is central to enabling authoritative DoD strategies while providing the vision for supporting strategies.

LINE OF EFFORT 1

Provide Joint Warfighting IT capabilities to expand strategic dominance of U.S. Forces & mission partners

Vision: Combined warfighting IT capabilities enables rapid, widespread sharing of information with mission partners and provides interoperability of our Joint Forces. Technologies must support all-domain operations, provide real-time intelligence, and allow all participants to share a common operational picture.

Overview: The warfighter requires advanced, secure, and interoperable IT that effectively supports the complex demands of the modern battlefield. The DoD must design and build capabilities that are functional, scalable, sustainable, and secure. Delivered capabilities must be user friendly and adaptable to the speed of warfare. The DoD must continue to reinforce alliances and partnerships with premier collaboration and data sharing capabilities. Interoperability with mission partners enables a swift and decisive response to any crisis, from any location, in any environment, and during any threat condition.

In today's hyperconnected world, trustworthy data is indispensable for achieving strategic dominance. Advanced analytics and Artificial Intelligence and Machine Learning (AI/ML) must assist and complement the warfighter with rapid integration and display of data. Proprietary interfaces must be replaced with modern Application Programming Interfaces (APIs) that are built to commercial industry standards.

STRATEGIC OBJECTIVES

- **1.1 Provide an intuitive and adaptive user experience**: *Ensure warfighters can quickly adapt and integrate technology into their jobs.*
- **1.2 Treat and secure data as a strategic product:** *Effectively harness data on, and in support of, the battlefield, leading to decisive action for our military to outmaneuver any threat.*
- **1.3 Harness advanced technologies for strategic advantage:** *Integrate advanced technology rapidly into warfighting systems.*
- **1.4 Outpace adversaries with Global C3 capabilities:** *Modernize U.S. warfighting IT capabilities to include electromagnetic spectrum capabilities that ensures warfighters and senior leaders can exercise superior command, control, and communications (C3).*

Strong cybersecurity mechanisms must be implemented according to Zero Trust (ZT) principles and intertwined with DoD software solutions and data to deter advanced persistent threats. Enterprise solutions for identity, credentialing, and access management (ICAM) are critical enablers for protecting data, user access, and APIs at an advanced level.

The warfighter must be equipped with functional and resilient applications and data that enhance Joint Command, Control, and Communication (C3) capabilities. To gain decisive advantage on the battlefield, it is equally important to bolster warfighter assurance globally in key technology enablers including positioning, navigation, and timing (PNT), electromagnetic spectrum (EMS), and National Leadership Command Capabilities (NLCC).

What success looks like

A seamlessly integrated digital ecosystem characterized by an intuitive UX, where the right users can access the right data, at the right time, for the right reason. Warfighters have access to modern applications to execute their missions. Advanced technologies, such as AI and ML have propelled the Department forward by enabling predictive analytics, automation of repetitive tasks, and the creation of personalized experiences.

A robust technology infrastructure forms the foundation for critical Departmental operations. Stringent security measures and protocols are implemented to safeguard data integrity, confidentiality, and availability across diverse communication platforms. The warfighter has freedom of action across multiple domains with access and shared information in contested, congested, and

constrained electromagnetic spectrum environments. Advanced encryption techniques and identity management solutions have been deployed to fortify the digital ecosystem against advanced cyber threats. Ultimately, deployment of advanced warfighting IT capabilities for joint forces and mission partners has improved decision and competitive advantage for swift and decisive responses to high-tempo, multi-domain operations.

How to measure progress

The following summary represents a collection of important considerations to focus on and measure progress against during the implementation of this strategy. Additional priorities may be added as implementation planning and delivery unfold.

1.1 Provide an intuitive and adaptive user experience

What to measure	Why it matters
1.1.1. Deliver Mission Partner Environment capabilities to support U.S. and mission partners.	Data sharing with mission partners enables joint force operations. Sharing relevant information improves situational awareness, fosters interoperability, and achieves broader impact and influence collectively.
1.1.2. Develop and deploy critical web-based mobility apps to warfighters and mission partners.	Current systems put too much friction and cognitive load with manual workarounds for the joint warfighter. Modern applications dramatically reduce decision time.
1.1.3. Reduce the number of systems that require separate logins and/or endpoints.	Forcing customers to "swivel chair" between different systems impacts mission effectiveness. Enabling interoperability across IT systems enhances productivity and UX.
1.1.4. Increase performance of managed DoD computers to comparable industry standards.	Improving system boot and run times increase productivity, facilitate update frequency, and enhance security. Long system boot times and run time performance issues are a symptom of multiple underlying tech refresh and operational issues.
1.1.5. Reduce time-to-resolution for service disruptions.	Reduction in time-to-resolution indicates improved efficiency in addressing IT issues, leading to increased productivity, and minimized disruption to mission operations.
1.1.6. Increase user satisfaction with IT services.	User satisfaction is a crucial indicator of overall IT effectiveness. A rise in satisfaction levels suggests that the service providers have successfully addressed user needs and expectations, resulting in a better UX.

1.2 Treat and secure data as a strategic product

What to measure	Why it matters
1.2.1. Replace proprietary data interfaces with modern APIs that are built to commercial industry standards and properly secured.	Open APIs facilitate data sharing by providing clearly documented and accessible interfaces that allow software applications to seamlessly exchange information.
1.2.2. Configure APIs to "apply the principle of least privilege".	Mitigate cybersecurity risk against attacks on open APIs. Users should only receive data enabled by dynamic need-to-know policy rules.
1.2.3. Increase monitoring for APIs and applications.	Rapidly detect and mitigate irregular user behavior, which may be an indicator of compromise or insider threat.
1.2.4. Increase data encryption at rest and in transit.	Encryption prevents data from falling into the wrong hands.
1.2.5. Transition operational systems to a secure, scalable, and resilient network of cloud and edge nodes.	Enables rapid processing of data at the tactical edge during disrupted, denied, intermittent, and limited (DDIL) conditions for informed decision-making.
1.2.6. Adopt enterprise ICAM shared services for use in DoD Systems.	Enables the right users (people, devices, or robotic processes) to access the right resource, at the right time, and for the right reason.
1.2.7. Advance protection of the Defense Industrial Base (DIB) Controlled Unclassified Information through adoption of Cybersecurity Maturity Model Certification program requirements.	Increased assurance that DIB contractors meet DoD cybersecurity contract requirements.

1.3 Harness advanced technologies for strategic advantage

What to measure	Why it matters
1.3.1. Apply AI/ML to real-time warfighting decision processes.	Application of AI/ML to warfighter decisions processes increases the speed and accuracy of information and enhances decision advantage.
1.3.2. Automate strategically relevant manual processes using Robotic Process Automation or AI/ML.	In leveraging automation where appropriate you are improving the ability of the warfighter to achieve and maintain competitive advantage.
1.3.3. Automate machine data tagging for strategically relevant systems.	Eliminates the laborious process of making data AI-ready and accelerates the application of AI to processes for decision advantage.
1.3.4. Complete end-user platforms cryptographic modernization and advanced cryptographic capability modifications.	Provides the warfighter with advanced cryptographic compliant tools eliminating the burden for end user modification and configuration.
1.3.5. Equip new Command and Control (C2) systems with built in cryptographic modernization capability and compatibility.	Crypto modernization protects the confidentially of the warfighter's critical data which prevents the exploitation of the data by an adversary.
1.3.6. Build in supply chain cyber security.	Ensuring the supply chain is secured provides flexibility to accelerate the acquisition of national security systems but also reduces injecting unnecessary system vulnerabilities.

1.4 Outpace adversaries with Global C3 capabilities

What to measure	Why it matters
1.4.1. Provide assured PNT as an enterprise service to the Joint Force.	Ensures secure and precise position, navigation, and timing to support high tempo multi-domain operations across a variety of Naval Information Warfare Systems Command environments.
1.4.2. Deploy an agile, integrated spectrum infrastructure and data environment.	Ensure freedom of action across multiple domains to access and share information to maneuver in a contested, congested, and constrained electromagnetic spectrum environment.
1.4.3. Field a modernized, secure, survivable senior leader video and voice conferencing system.	Provides diverse, accurate, integrated, survivable, secure, and timely assured communication pathways allowing national leadership to execute command responsibilities throughout the escalation conflict.
1.4.4. Enhance terrestrial, maritime, space, and aerial transport infrastructure.	Assures accessibility of cloud-based applications, data, and communications for the warfighter at the tactical edge.
1.4.5. Implement Defense Regional Clocks (DRC) global ring.	Improve the endurability and availability of critical time for mission critical systems and applications.
1.4.6. Integrate and centralize NLCC Enterprise Management.	Improves alignment and synchronization of nuclear command, control, and communications (NC3), continuity of operations planning (COOP), continuity of government (COG), and senior leader communications architectures.
1.4.7. Implement Enterprise Satellite Communications (SATCOM) Management and Control (ESC-MC) to improve resilience and resource allocation agility.	Increase resiliency by providing the warfighter with rapid communication avenues.

LINE OF EFFORT 2

Modernize information networks and compute to rapidly meet mission and business needs

Vision: DoD information networks will fully leverage the power and versatility of commercial information technology and evolve from a network-centric security paradigm to a data-centric, ZT model.

Overview: The Department stands in a new era defined by unprecedented technological advancement and global interconnectedness. The imperative to modernize our global information networks and compute fabric has never been more urgent. The DoD information enterprise is at the center of military operations, enabling communication, coordination, and decision-making across the range of conflict: strategic, operational, and tactical.

The modern warfighter requires IT infrastructure that can process and disseminate vast amounts of data reliably and rapidly from anywhere in the world. Highly resilient, survivable, scalable, and secure IT assets are critical to maintaining strategic dominance in a globally competitive landscape. The challenges the Department faces in the digital age are immense and multifaceted. Legacy systems, disparate networks, and outdated technologies have created bottlenecks and vulnerabilities that threaten to undermine our readiness and resilience.

Global dynamic resilience of our IT infrastructure requires both scalability and survivability. Pushing towards enterprise commercial multi-cloud environments across all classification levels will offer global compute and hyperscale networking will offer the DoD ready access to industry innovation at a pace unattainable by the DoD alone.

Cybersecurity is a key aspect of this future global enterprise. The pace of technological innovation has accelerated exponentially, and our adversaries leverage emerging technologies to exploit weaknesses and gain strategic advantage. Implementation of ZT across information networks and computers mean that the Department will not be solely reliant on perimeter-based defenses; all hosts will be treated as though they are compromised and hostile. Continuous monitoring, automated alerts and security responses will be incorporated into the fabric of the DoD information enterprise.

STRATEGIC OBJECTIVES

- **2.1 Optimize the DoD Information Network (DoDIN) foundation:** *Remediate existing technical debt and legacy technologies across the DoDIN to improve performance and user experience. Integrate and simplify disparate DoD networks and compute capabilities.*
- **2.2 Enable global dynamic resilience:** *Transform the DoDIN with an intentional network architecture that leverages the best-in-class technology, and emerging capabilities as they become available.*
- **2.3 Implement ZT across DoD networks and compute fabric:** *Secure networks and compute fabric with ZT to increase resiliency against threats across the full range of conflict.*

What success looks like

A modernized, information network that is a dynamic and agile ecosystem leveraging best-in-class technologies enabling faster data transfer, lower latency, and greater network capacity. Technical debt (TD) and legacy constraints have been minimized, and DoD networks and compute fabric exceed the dynamic and global needs of the Department. Implementation of next generation technology (e.g., 5G) and modernized SATCOM are providing advanced global transport connectivity at tactical edge, additional network capacity, and a high degree of resiliency for the Warfighter.

Implementation of ZT security is providing comprehensive protection against cyber threats by continuously verifying user identities and scrutinizing network traffic, thereby fortifying the network's defenses.

How to measure progress

The following summary represents a collection of important considerations to focus on and measure progress against during the implementation of this strategy. Additional priorities may be added as implementation planning and delivery unfold.

2.1 Optimize the DoDIN foundation

What to measure	Why it matters
2.1.1. Reduce legacy networks and technologies across the enterprise.	Elimination of legacy technologies reduces costs, improves interoperability, reduces cybersecurity threats, and improves resource allocation.
2.1.2. Reduce latency across virtual or physical network and boundary devices.	Simplified network configuration increases network performance and UX.
2.1.3. Reduce TD ratio across the Department.	Reduction in TD ensures that the network and compute infrastructure is maintainable, scalable, and able to meet the changing needs of users.

2.2 Enable global dynamic resilience

What to measure	Why it matters
2.2.1. Expand the use of cloud service providers (CSPs).	CSPs provide scalability across all classification levels.
2.2.2. Increase Joint Operational Edge (JOE) nodes globally.	Enable rapid compute and data processing at the edge while supporting caching of data in DDIL conditions.
2.2.3. Increase Outside the Continental U.S. (OCONUS) on-premises cloud capabilities (e.g., Stratus).	Complement commercial cloud computing with DoD-owned and operated cloud services.
2.2.4. Create consolidated information domains and network entry points for mission partners (international, inter-agency, and DIB).	Enables rapid mission partner accessibility of data, while minimizing operational overhead and threat surface.
2.2.5. Modernize and transform the network ecosystem supporting national security systems.	Modernization of the networking ecosystem for national security systems will improve cybersecurity, UX, increase resiliency, and scalability.
2.2.6. Implement 5G across DoD installations and operating forces.	Increases network capacity and enhances reliable connectivity for simultaneously connected devices with diverse usage patterns.
2.2.7. Improve C3 capabilities and survivability at the tactical edge.	Secure and resilient C3 capabilities are essential for assured and trusted battlefield information exchange.
2.2.8. Modernize enterprise DoD public safety communications capabilities.	Improves emergency management and force protection response time. Allows for integration of advanced security features and provides the flexibility to incorporate emerging technologies to ensure effective emergency response, coordination between emergency managers, and improved situational awareness.

2.3 Implement ZT across DoD networks and compute fabric

What to measure	Why it matters
2.3.1. DoD Components achieve ZT "target level" requirements for User (ZT User Pillar).	Strong authentication helps ensure that only authorized individuals and entities can access sensitive data and resources. Prevents unauthorized users and malicious actors from gaining access and compromising security.
2.3.2. DoD Components achieve ZT "target level" requirements for devices (ZT Device Pillar).	Proactively mitigate unauthorized access and address device vulnerabilities that could be exploited by cyber attackers.
2.3.3. DoD Components achieve ZT "target level" requirements for applications, systems, and workloads (ZT Applications, Systems, and Workloads Pillar).	Embed security throughout the rapid development and deployment of applications and systems.
2.3.4. DoD Components achieve ZT "target level" requirements for data (ZT Data Pillar).	Ensures that data is handled and protected according to its sensitivity level, regulatory requirements, and business needs. Robust end-to-end encryption ensures that data remains secure and confidential, even if intercepted by unauthorized parties.
2.3.5. DoD Components achieve ZT "target level" requirements for enterprise networks (ZT Networking Pillar).	Proactively mitigates advancements in cybersecurity threats by taking an "never trust, always verify" approach to the networks.
2.3.6. DoD Components achieve ZT "target level" requirements for automation and orchestration (ZT Automation & Orchestration Pillar).	Ensures rapid response to security events in real-time for improved threat detection and mitigation. Automation minimizes the impact of security incidents and improves prevention of data breaches or system compromises.
2.3.7. DoD Components achieve ZT "target level" requirements for visibility and analytics (ZT Visibility & Analytics Pillar).	Enhances threat detection by identifying patterns indicative of potential security threats that may go unnoticed by traditional rule-based systems. Differentiates between normal behavior and abnormal or malicious activity, enabling better understanding of the nature and severity of potential threats.
2.3.8. Increase logging and improve certified cloud security professional visibility into the cyber security status and alerts generated.	Rapidly identify and proactively respond to evolving threats in the DoD hybrid-cloud environment.

LINE OF EFFORT 3

Optimize IT Governance to gain efficiencies in capability delivery and enable cost savings

Vision: Enhance IT management and oversight to ensure that resources are utilized effectively and aligned with mission objectives at the speed of warfare.

Overview: The Department is continuing a transformative journey to revolutionize IT for the modern battlefield. Fueled by the commitment to equip the total force with cutting-edge capabilities, DoD will overhaul governance with streamlined policies, processes, efficient allocation of resources, continuous monitoring, and evaluation of IT performance.

Robust data improves the effectiveness of IT governance. Decision makers must be able to trust, understand, and use IT data to identify tradeoffs, make critical decisions, and manage risk.

Streamlined Defense Business Systems (DBS) and enterprise IT leverages economies of scale by consolidating resources and eliminating legacy systems. Governance frameworks prioritizes DBS portfolio rationalization. Legacy systems that no longer support business objectives or incur high maintenance costs are targeted for consolidation, elimination, or replacement with more efficient alternatives.

DoD will streamline acquisition and embrace Developer Security Operations (DevSecOps) to bridge the gap from requirement to deployment while ensuring cybersecurity remains paramount throughout sustainment.

IT governance serves as the cornerstone for driving departmental success in today's rapidly evolving landscape. By providing the framework and oversight needed to align IT resources with strategic objectives, the Department is empowered to fully maximize operational efficiency and impact.

STRATEGIC OBJECTIVES

3.1 Overhaul IT governance process and tools for Department-wide implementation: *Streamline IT governance to result in faster and clearer decision-making across the Department's IT Portfolio.*

3.2 Use trusted and curated data to advance IT Governance: *Arm decision-makers with high quality, trusted data, and architectures required to make critical decisions on the DoD IT portfolio and rationalize risk.*

3.3 Streamline Defense Business Systems and Enterprise IT: *Transform the Defense Business Systems portfolio and drive toward enterprise IT solutions that result in economies of scale for the Department.*

3.4 Accelerate acquisition, development, and deployment of IT: *Streamline IT processes, enabling the Department to serve the warfighter and broader DoD enterprise.*

What success looks like

A unified governance structure that aligns with organizational objectives fostering efficiency and innovation. A cohesive governance framework is in place that standardizes policies, processes, and procedures across all IT operations. A common data framework has been implemented and driving business outcomes by ensuring consistency, accuracy, and accessibility of data products that facilitate informed decision-making. Duplicative and obsolete DBSs have been consolidated or eliminated, while relevant legacy DBSs have been modernized to maximize cost-effectiveness. IT acquisitions have been streamlined accelerating the deployment of technology solutions enabling rapid adaptation to mission requirements.

How to measure progress

The following summary represents a collection of important considerations to focus on and measure progress against during the implementation of this strategy. Additional priorities may be added as implementation planning and delivery unfold.

3.1 Overhaul IT governance process and tools for Department-wide implementation

What to measure	Why it matters
3.1.1. Construct a comprehensive, unified IT governance framework which reduces duplication.	Provides streamlined decision-making for efficiency and clarity across the Department's IT portfolio.
3.1.2. Foster data-driven and automated methods of governance for compliance decisions/analysis.	Maturation of the Department's data and decision-making process drive improved governance efficiencies.
3.1.3. Identify and address policy constraints that inhibit optimization of DoD IT systems.	Removing policy roadblocks and constraints simplifies governance and optimizes the IT ecosystem.

3.2 Use trusted and curated data to advance IT governance

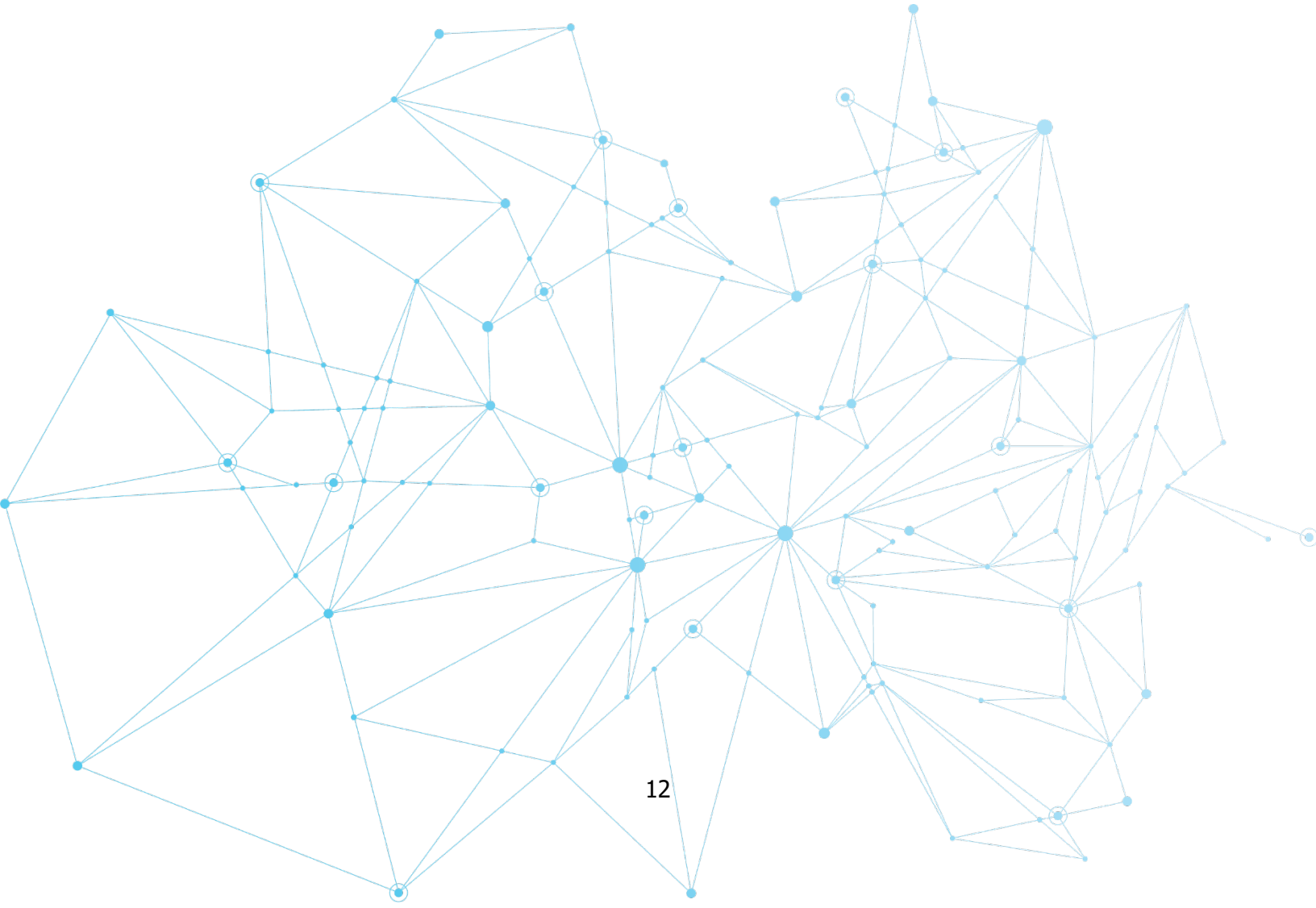
What to measure	Why it matters
3.2.1. Enhance data interoperability.	Improves interoperability ensuring data generated by one system can be easily understood and used by another without extensive translation or transformation.
3.2.2. Increase use of IT data standards of core data entities. (e.g., system, application, software, etc.).	Adherence to data standards ensures trustworthiness and quality of data for decision-makers.
3.2.3. Increase data quality across authoritative sources.	Increasing quality, including metadata, enables IT data citizenship while ensuring IT data is curated, trusted, and available to make effective decisions.
3.2.4. Improve use of data tags and metadata.	Tagging of metadata enables structured data decision automation.
3.2.5. Increase automation of Records Management (RM).	Automation reduces human error, manual processes, and the recordkeeping burden on IT customers and endpoint users.
3.2.6. Increase accessibility of DoD electronic and IT for users with disabilities.	Ensures equal access of government information systems, electronic content, and websites for users with disabilities.
3.2.7. Improve curation of data.	Providing trustworthy information to decision makers results in timely and informed decision-making.

3.3 Streamline Defense Business Systems and Enterprise IT

What to measure	Why it matters
3.3.1. Increase the pace of DBS rationalization.	Ensures cost avoidance by eliminating resources required to maintain legacy systems.
3.3.2. Decrease number of duplicative capabilities across DBS and IT infrastructure.	Ensures cost avoidance by eliminating resources required to maintain duplicative systems.
3.3.3. Increase adoption of DoD wide enterprise IT services, contracts, and systems for higher efficiencies.	Efficiency gains (i.e., cost, contract award time, delivery time) across the Department due to increased adoption of enterprise IT services.

3.4 Accelerate acquisition, development, and deployment of IT

What to measure	Why it matters
3.4.1. Reduce delivery cycle timeline.	Identifies opportunities for capability delivery process improvement while reducing delivery cycle time.
3.4.2. Increase the number of programs leveraging continuous Authorization to Operate (cATO) for faster delivery.	Leveraging agile, DevSecOps processes, and capabilities shortens delivery cycles while delivering secure capabilities.
3.4.3. Increase use of common architecture, risk frameworks, and standards.	Provides the foundation for DoD Components and DIB partners to build to, reducing inefficiencies and shortening integration time.



LINE OF EFFORT 4

Cultivate a premier digital workforce ready to deploy emerging technology to the warfighter

Vision: Shape a highly skilled digital workforce equipped with the latest knowledge and expertise, poised to swiftly deploy emerging technologies and drive innovation.

Overview: The DoD must continue to identify, recruit, develop, and retain talent that is driven by purposeful work, and that feel connected to the greater cause of the national security mission. This essential workforce encompasses a wide range of activities and technologies that includes IT, cybersecurity, cyber effects, intelligence, and enabler work roles within the DoD Cyber Workforce Framework (DCWF). The Department is broadening the DCWF to include data, AI, software engineering, transitioning into the digital workforce. The digital workforce is cross-cutting and inclusive of those who support functions across human resources, finance, logistics and many other functional activities.

Investment in our workforce is critical to the success of the Department's ability to deliver technology to the warfighter. The DoD workforce serves as the backbone of our digital infrastructure, possessing the expertise to develop, maintain, and secure the technology systems that drive efficiency, innovation, and competitive advantage in today's modern battlefield. As technology continues to evolve rapidly, ongoing investment in IT professionals ensures that the Department can adapt to emerging trends, mitigate cybersecurity risks, and capitalize on new opportunities.

STRATEGIC OBJECTIVES

4.1 Build a top-tier digital workforce: *Identify and recruit top talent to ensure the DoD has skilled personnel equipped to integrate and deploy technology for the Department.*

4.2 Prioritize continuous learning for the digital workforce: *Invest in opportunities for the workforce to remain current and keep pace with new and emerging technology, trends, and mission needs.*

4.3 Retain an exceptional digital workforce: *Offer a compelling workplace so that the DoD is seen as an employer of choice across the federal government.*

4.4 Foster collaborative partnerships to enhance the digital workforce: *Prioritize partnerships across government, industry, and academia to enhance capability, development, and effectiveness.*

In a highly competitive employment landscape, the DoD must be seen as an employer of choice across the Federal Government and industry. To attract, recruit, and retain an exceptional digital workforce, the Department must offer competitive compensation, work-life balance, continuous learning opportunities, career development, functional workspaces, and innovative environments with flexibility in when and where people work.

The Department must increase the use of non-traditional hiring authorities for critical work roles while minimizing timelines to on-board new employees. Infusion of new talent, educated on the latest technologies, will be pursued through entry level scholarship programs, university outreach, partnerships with academia, industry experts, and technology communities.

Cultivating a premier digital workforce is paramount for the success and sustainability of the Department. By investing in identifying, recruiting, developing, and retaining top talent, organizations can build a culture of excellence, collaboration, and continuous improvement. An empowered digital workforce not only delivers exceptional results but also serves as a catalyst for positive change and long-term success.

What success looks like

A fulfilled, engaged, and productive digital workforce, inspired by a diverse cadre of visionary leaders deeply committed to the success of our mission. These professionals are delivering world-class digital capabilities to the warfighter in a relevant and timely manner. The DoD digital workforce is characterized by informed critical thinkers at the strategic, operational, and tactical level. The DoD is actively recruiting talented, highly skilled, and impassioned individuals from diverse backgrounds and experiences.

Our digital workforce is engaged and learning through academic experiences, mentorships, and developmental opportunities. Employees have hybrid flexibility in where and when they work. They have state-of-the-art tools that enable remote work and virtual collaboration.

Career paths are clear yet flexible, and succession planning helps organizations cultivate the next generation of digital leadership. Staff are empowered to identify, evaluate, and act to solve problems. Prudent risk taking is celebrated, and performance reviews reflect impact. As a result, employee satisfaction is high and digital professionals at all levels are leaders, able to support decisions that optimize mission execution.

How to measure progress

The following summary represents a collection of important considerations to focus on and measure progress against during the implementation of this strategy. Additional priorities may be added as implementation planning and delivery unfold.

4.1 Build a top tier digital workforce

What to measure	Why it matters
4.1.1. Increase digital occupation billets coded IAW DoD Cyber Workforce Framework (DCWF) in manpower system(s) of record.	Enables the Department to assess readiness and shape recruitment efforts.
4.1.2. Increase digital occupation personnel coded IAW DCWF in personnel system(s).	Provides data to support workforce management including development of digital career paths, recruiting, retention, and talent management initiatives.
4.1.3. Decrease the DCWF digital occupations time-to-hire.	Prolonged hiring times increase the likelihood that DoD will lose desired digital workforce talent to other employers.
4.1.4. Use non-traditional hiring authorities for critical DCWF work roles.	Enables expedited hiring, targeted recruiting and outreach for critical workforce needs thereby improving the ability to attract top candidates.
4.1.5. Increase utilization of DoD-sponsored entry-level hiring programs.	Brings in fresh ideas, enables succession planning, infuses more long-term growth, and stability into the digital workforce to reduce attrition rates.

4.2 Prioritize continuous learning for the digital workforce

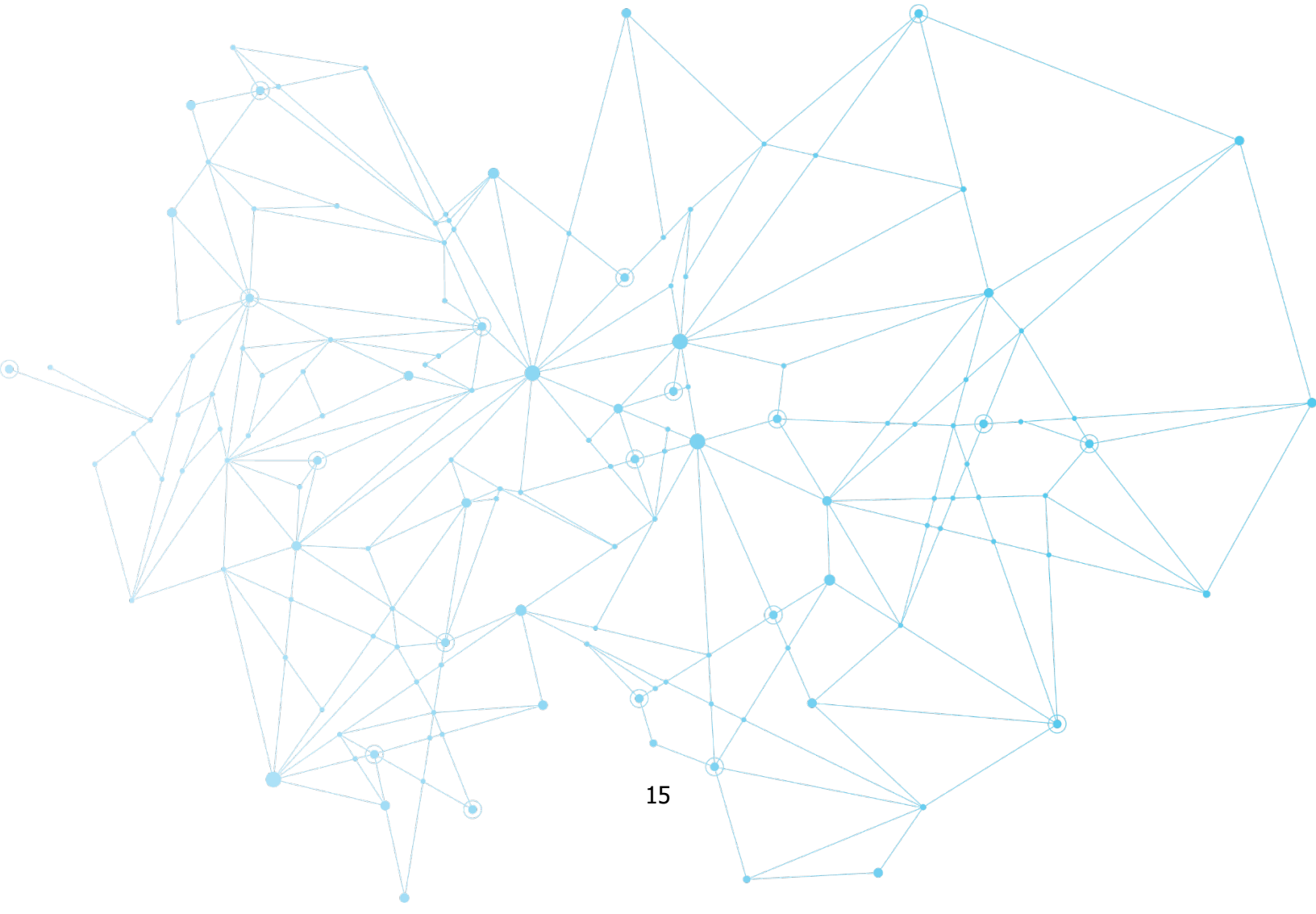
What to measure	Why it matters
4.2.1. Qualify the digital workforce in accordance with the Cyberspace Workforce Qualification and Management Program requirement set forth with DOD Manual 8140.03 (8140 Program)	The 8140 Program specifies the enterprise baseline qualification requirements by work role needed to enhance mission readiness. Regular updates to these requirements based on technology trends and mission needs ensure the workforce remains current to keep pace with technology. Data about the proficiency of the cyber workforce informs assignment, training, and career development decisions.
4.2.2. Increase participation in sponsored professional development opportunities.	DoD-sponsored professional development opportunities (e.g., Naval Postgraduate School, Air Force Institute of Technology, National Defense University, Executive Leadership Development Program) reflect the importance placed on a culture of continuous learning by the Department.

4.3 Retain an exceptional digital workforce

What to measure	Why it matters
4.3.1. Increase job satisfaction across the digital workforce.	To attract, recruit, and retain a digital workforce in today's competitive environment, the Department must offer competitive compensation, work-life balance, job stability, functional work location, innovative environment, and flexibility in when and where people work.
4.3.2. Increase the rate of retention of scholarship participants beyond initial service for each cohort.	Fostering an environment that prioritizes the return on investment of digital workforce opportunities (e.g., scholarship, developmental) will demonstrate the Department's commitment to retaining top talent and encouraging a culture of innovation.

4.4 Foster collaborative partnerships to enhance the digital workforce

What to measure	Why it matters
4.4.1. Increase rotation and exchange program participation.	Rotational assignments offer opportunities to immerse the digital workforce in diverse experiences strengthening the knowledge base and fostering a culture of personal and professional growth.
4.4.2. Increase the number of partnerships (e.g., commercial, federal, academic) established through memorandums of understanding and other documents.	Mature and stable partnerships are a crucial force multiplier and help identify both emerging technology and talent.



From Strategy to Outcomes

Fulcrum describes “what” the DoD must achieve with respect to advancing IT for the warfighter and “why” it matters. The detailed implementation plan required to achieve these goals and objectives will describe the “how” we will get there. It is forthcoming as part of our immediate next steps. The CIO will establish a governance forum that meets regularly to manage the collective priorities outlined in this strategy, track delivery, and focus resources in support of driving to the intended outcomes.

Archimedes, a mathematician, and inventor in ancient Greece, was reported to have said, “Give me a lever long enough and a fulcrum on which to place it, and I shall move the world.” This strategy serves as the fulcrum for empowering DoD leaders to drive transformative change and advance technology for the warfighter in an evolving world. We must continue to work in partnership across the Department to fully realize these outcomes.