DISA STRATEGIC PLAN

2019 - 2022
Version 1

A Letter from the Director

The Defense Information Systems Agency (DISA) is the department's premier information technology provider and is committed to being the trusted provider to connect and protect the warfighter in cyberspace, while Joint Force Headquarters - DOD Information Network (JFHQ-DODIN) is laser-focused on maintaining command and control (C2) of defensive cyber operations. As both the director of DISA and commander of JFHQ-DODIN, I am honored to lead two organizations with distinct but complementary missions.

Together, as Department of Defense employees, we occupy a distinct position of trust with the American people. This position of trust requires a strong ethical and moral compass and allows us the honor of serving our nation, supporting the warfighter, and achieving our mission. We have a tough challenge ahead as we confront near-peer threats in the cyberspace domain. It requires the agility, response, and resilience of the entire team to ensure DISA is postured to support the Department of Defense.

This four-year plan focuses on our future within the Department of Defense and the ever-changing cyberspace environment. It focuses on developing and reinforcing trusted partnerships to connect and protect the warfighter in cyberspace while contributing to the lethality of our joint fighting force. The strategic goals and objectives are a framework to provide, operate, and assure C2 and information-sharing capabilities in direct support of joint warfighters, national-level leaders, and other mission and coalition partners across the spectrum of military operations.

Nancy A Norton

NANCY A. NORTON
Vice Admiral, USN
Director/Commander

Table of Contents

A Letter from the Director	3
Table of Contents	4
Executive Summary	5-6
Context	7
Strategic Framework	8-9
Guiding Principles	10
Technology Roadmap	11
Strategic Goals and Objectives	12-17
Goal 1: Operate and Defend	12-13
Goal 2: Adopt, Buy, and Create Solutions	14-15
Goal 3: Enable People and Reform the Agency	16-17
Conclusion	18
References	

Executive Summary

The DISA and JFHQ-DODIN fiscal year (FY) 2019 – 2022 Strategic Plan provides the framework to complete our respective missions in support of the Department of Defense (DOD). Our mission is to conduct DODIN operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation. This mission supports the National Defense Strategy's three lines of effort to restore military readiness as we build a more lethal force, strengthen our alliances and build new partnerships, and drive business reforms for innovation and modernization. To accomplish our mission and achieve these efforts, we developed three goals and seven strategic objectives. The three goals are: operate and defend; adopt, buy, and create solutions; and enable people and reform the agency. The seven strategic objectives are: modernize the infrastructure, enhance operations, optimize for the enterprise, strengthen cybersecurity, drive innovation, enable people, and reform the agency.

DISA's mission, vision, values, creed, and ethos serve as enduring principles to guide our dedicated team of military, civilian, and contract personnel in day-to-day operations. It is our vision to be the trusted provider to connect and protect the warfighter in cyberspace for decades to come. Our core values are **D**uty that **I**nspires **S**ervice and **A**ccountability, and our creed is to unite diversity of **T**alent through **R**espect, **U**nity, **S**ervice, and **T**eamwork, leading innovation and success for the warfighter in defense of our nation. At the core of our guiding statements is our ethos, "Trust in DISA: Mission First, People Always!"

The Strategic Plan is an overarching framework that informs planning priorities, resource allocation, and assessment criteria. The alignment and synchronization of priorities, resources, and assessments ensure we achieve the highest levels of performance and productivity on an enduring basis.

The Strategic Plan framework holistically supports the joint forces' ability to win against any adversary, the agility to adapt to any challenge, the endurance to sustain any campaign, the resilience to recover readiness quickly, and the flexibility to address multiple challenges under different conditions. DISA and JFHQ-DODIN will review and update the strategic plan at the beginning of each fiscal year to ensure the services and capabilities provided contribute to a more lethal, resilient, and innovative joint force.

Context

Strategies aimed at improving the national defense posture continue to evolve. The DOD's long-term cyber strategic approach is based on mutually reinforcing lines of effort to build a more lethal joint force, compete and deter in cyberspace, expand alliances and partnerships, reform the department, and cultivate talent.

The National Security Strategy, National Cyber Strategy, National Defense Strategy, National Defense Business Operations Plan, National Military Strategy, DOD Cyber Strategy, and DOD Digital Modernization Strategy align with or support the DOD.

New strategies that address technology adoption include the DOD Artificial Intelligence (AI) Strategy and the DOD Cloud Strategy. The AI strategy outlines the requirement for speed and agility to translate artificial intelligence into operationally relevant military capabilities at the rate of technological advancement. The cloud strategy outlines the need for a secure cloud environment that spans to the tactical edge and is capable of providing rapid computing and storage capacity.

Collectively, these strategies guided the development of the strategic plan and support the DOD's goal to strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. The strategic plan highlights efforts to improve our mission partner's customer service experience in a more transparent, effective, and efficient way.

Strategic Framework

The strategic framework shows how the guiding principles, strategic capabilities, strategic objectives, and strategic goals support the agency's mission of conducting DODIN operations to enable lethality across all warfighting domains in defense of our Nation.

The guiding principles to improve customer service, collaborate to innovate, measure what matters, and take prudent risks are enduring philosophies to accomplish the objectives and goals.

The capabilities are the programs, projects, and initiatives that support the objectives.

The objectives are the actions taken to achieve the goals, and the goals support our enduring mission.

DISA Mission

To conduct DODIN operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation.

DISA Vision

To be the trusted provider to connect and protect the warfighter in cyberspace.

DISA Values

Duty that Inspires Service and Accountability

DISA Creed

We are a combat support agency. We unite diversity of *Talent* through *Respect, Unity, Service,* and *Teamwork*, leading innovation and success for the warfighter in defense of our Nation.

DISA Ethos

Trust in DISA – Mission First, People Always

Strategic Goals

Operate and Defend	Adopt, Buy, and Create Solutions	Enable People & Reform the Agency

Strategic Objectives

1.1 Modernize the Infrastructure 1.2 Enhance Operations	2.1 Optimize for the Enterprise 2.2 Strengthen Cybersecurity 2.3 Drive Innovation	3.1 Enable People 3.2 Reform the Agency

Strategic Capabilities

1.1 Modernize the Infrastructure

- 1.1.1 Network Enhancements
- 1.1.2 Legacy Elimination
- 1.1.3 Internet Protocol v6
- 1.1.4 Fourth Estate Network / Data Center Consolidation
- 1.1.5 Spectrum Modernization
- 1.1.6 Joint Information Environment
- 1.1.7 Survivable Infrastructure
- 1.1.8 Satellite Communications Modernization
- 1.1.9 Software Defined Enterprise

1.2 Enhance Operations

- 1.2.1 Network Operations
- 1.2.2 Defensive Cyber Operations – Internal Defensive Measures
- 1.2.3 Mission/Quality Assurance & Critical Infrastructure
- 1.2.4 Defense Industrial Base
- 1.2.5 Exercises and Training
- 1.2.6 Contingency Plans
- 1.2.7 Ecosystem
- 1.2.8 Active-Active
- 1.2.9 Airborne Intelligence Surveillance & Reconnaissance
- 1.2.10 Special Access Programs
- 1.2.11 Assessments
- 1.2.12 National Leadership Command Capability

2.1 Optimize for the Enterprise

- 2.1.1 milCloud 2.0
- 2.1.2 Unified Capabilities
- 2.1.3 C2 Portfolio
- 2.1.4 Mobility Offering
- 2.1.5 IT Tools Reform and Consolidation

2.2 Strengthen Cybersecurity

- 2.2.1 Cybersecurity Service Provider
- 2.2.2 Artificial Intelligence
- 2.2.3 Machine Learning
- 2.2.4 Identity Credential Access Management/Assured Identity
- 2.2.5 Endpoint Security
- 2.2.6 Comply-to-Connect

2.3 Drive Innovation

- 2.3.1 Development, Security, Operations/Agile Software Development
- 2.3.2 Acquisition Strategies
- 2.3.3 Partnerships Across DoD
- 2.3.4 Mobile/Desktop Convergence
- 2.3.5 Agile Software Development
- 2.3.6 Universal Transport

3.1 Enable People

- 3.1.1 Trust and Accountability
- 3.1.2 Culture and Reputation
- 3.1.3 Recruiting
- 3.1.4 Hiring
- 3.1.5 Training
- 3.1.6 Retention
- 3.1.7 Cyber Workforce
- 3.1.8 Acquisition Workforce
- 3.1.9 Equal Opportunity
- 3.1.10 Total Force Fitness Framework

3.2 Reform the Agency

- 3.2.1 DOD IT Reform
- 3.2.2 Internal Business Systems and Processes
- 3.2.3 Audit Readiness
- 3.2.4 Financial Systems
- 3.2.5 Testing
- 3.2.6 Customer Service
- 3.2.7 Provisioning Timelines
- 3.2.8 Joint Enterprise License Agreements

Guiding Principles

Improve Customer Service - Collaborate to Innovate - Measure What Matters - Take Prudent Risks

Guiding Principles:

Guiding principles serve as a broad philosophy to guide the accomplishment of all strategic objectives and goals. DISA and JFHQ-DODIN's four guiding principles are: improve customer service, collaborate to innovate, measure what matters, and take prudent risks.

Improve Customer Service

Improve the customer service experience to build trusted partnerships with our mission partners. This experience starts with an intuitive, reliable, and responsive request process, and ends with a well-built and tested service or capability. The end-to-end customer service experience is forged through transparency and trust. It also includes service to each other - treating teammates with equal consideration and trust to contribute to overall mission accomplishment.

Collaborate To Innovate

Drive the collaborative and innovative process by seeking new ideas and implementing new ways of doing business that lead to growth and improvement. The repurposing, redeveloping, integrating, and adapting of existing services, capabilities, and processes are also innovative ways to conduct business.

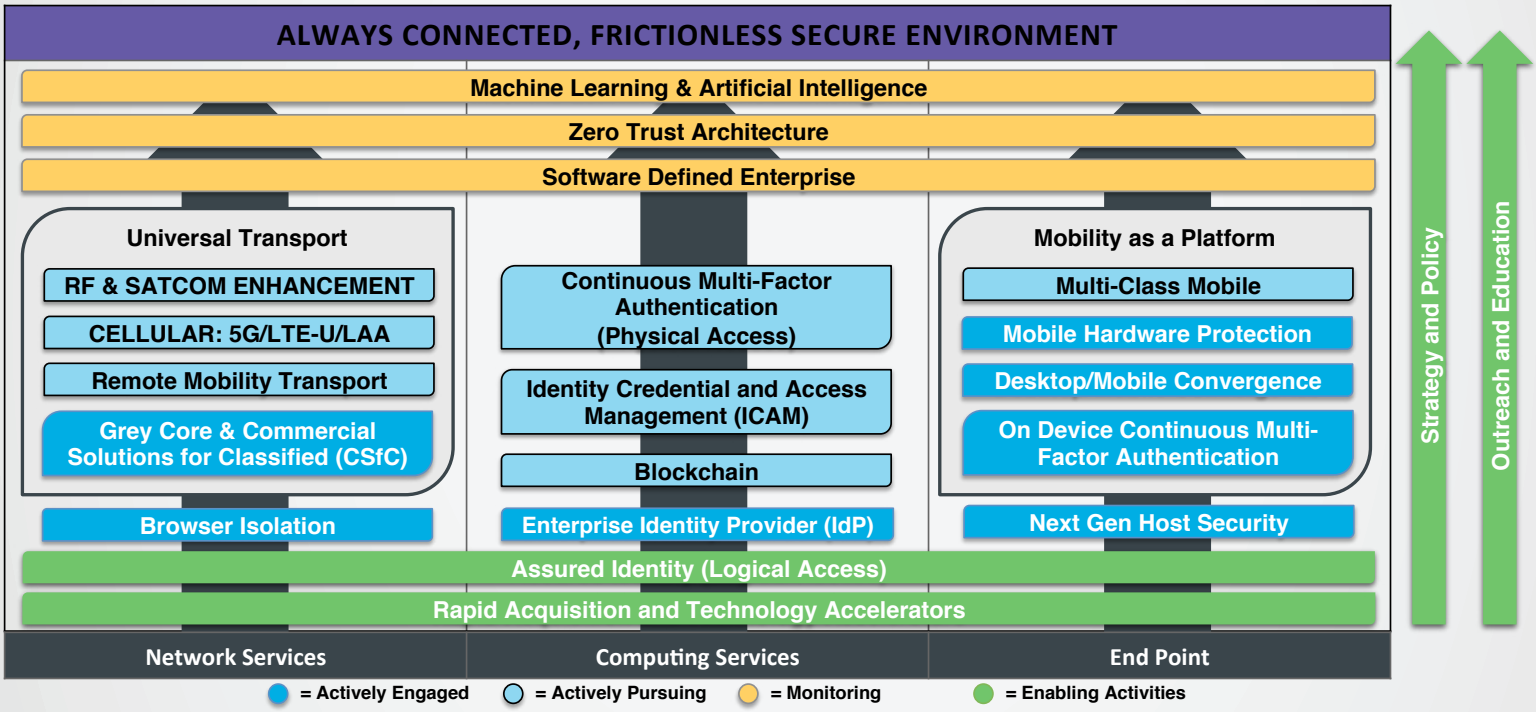
Measure What Matters

Develop and use metrics to measure application, service, and overall mission performance. DISA and JFHQ-DODIN's core missions and functions are aligned through the Defense Readiness Reporting System and the Management Internal Controls Program. Proactive and accurate readiness reporting reflects the agency's performance and effectiveness and promotes transparency and trust.

Take Prudent Risks

Practice the skill of assessing risks to ensure compliance with applicable laws, policies, issuances, and regulations. Practice taking prudent risks and transition from a "zero defect" culture to one that fosters agility and innovation. Prudent risk should be both encouraged and underwritten by the supervisory chain and contribute to providing the best solutions for our mission partners.

Technology Roadmap:



The technology roadmap describes the path DISA will use to achieve the goals and objectives outlined in the strategic plan. It provides a framework to explore technologies that will contribute to a more secure, coordinated, seamless, transparent, and cost-effective architecture for the DOD that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat.

The enabling activities provide speed and agility needed to translate new technologies into relevant military capabilities for the joint warfighter to enable lethality across all warfighting domains in defense of the Nation. Through a combination of outreach and education with mission partners, industry, academia, and our allies; effecting changes in DOD-level strategy and policy; rapid acquisitions; and the implementation of identity-based access, DISA improves the delivery timeline of innovative services and capabilities for mission partners.

By building trusted partnerships with our mission partners through regular engagement and collaboration, DISA strengthens customer service and its understanding of evolving mission partner priorities to deliver superior and secure capability to leaders and warfighters around the world. The stages of development for technologies ensure DISA is transparent in its activities and is driving innovation that anticipates emerging mission partner requirements, as well as increases IT performance and affordability for the DOD. It further ensures the allocation of resources to meet the mission partner requirements at the speed of relevance.

Strategic Goals and Objectives

Strategic Goal 1 | Operate and Defend

An era of technological advancement in the cyber domain is heightening the demand for responsive, resilient, secure, and high-quality IT services. DISA and JFHQ-DODIN understand these needs and recognize that in today's landscape of increasing cyber threats, the ability to deliver services and capabilities to customers across all domains – land, air, sea, space, and cyberspace – allows mission partners to maintain global leadership and deny unwanted advantages to adversaries. DISA is on the leading edge of deploying, operating, and sustaining cyber tools, capabilities, and expertise to maximize DODIN operations.

Strategic Objective 1.1 | Modernize the Infrastructure

DISA modernizes the infrastructure to improve the security, resiliency, and capacity for DOD networks. Modernization initiatives include standardized configurations, higher capacity, lower costs, and consolidating and converging data centers, networks, service desks, and network operation centers into a secure, integrated, and improved environment. A modern infrastructure reduces the cost and complexity to operate while improving customer service with standardization and transparency.

• Implement transformational initiatives required to modernize and evolve the Joint Information Environment construct to support dynamic DOD mission requirements and priorities. Support an everything-over-internet protocol (IP) architecture to eliminate obsolete technology, optimize network efficiencies and service delivery, and provide multi-path survivable infrastructure.

• Employ a global converged network infrastructure by converting to an IP-based architecture and implement Internet Protocol v6, where fault isolation and dynamic routing of network traffic enable enhanced service delivery and prevent service interruption to the end user. A global converged network infrastructure improves interoperability, security, resilience, and compliance with DOD net-centric directives and lowers sustainment costs while enhancing responsiveness to new requirements.

• Implement an agile, intelligent, and virtualized next-generation architecture that is secure-by-design through implementing next-generation identity and management solutions, comply-to-connect technologies, and a software-defined enterprise to enable a data-centric model that optimizes DOD-wide effectiveness and interoperability.

• Transform DOD joint electromagnetic spectrum operations through the implementation of holistic spectrum situational awareness to enable more dynamic spectrum operations and maneuver that enables greater lethality and survivability for spectrum-dependent systems supporting the wireless portion of the DODIN. Develop technical frameworks that enable promising new electromagnetic spectrum access technologies to provide improved full-range spectrum access for the warfighter.

Strategic Objective 1.2 | Enhance Operations

DISA enhances operations to ensure mission partners have secure, available, and reliable services and capabilities to achieve their mission in a contested cyberspace environment. DISA enhances operations through the operation and defense of the DISA-managed portion of the DODIN, management of the Cyber Security Service Provider program, support to combatant commands, and support of JFHQ-DODIN and U.S. Cyber Command in their mission to achieve cyberspace superiority.

• Enhance operations by developing a comprehensive network operations toolset used to monitor the status of the enterprise infrastructure, command and control (C2) networks, and information-sharing capabilities to provide resolution of network anomalies or interruptions.

• Expand resiliency through the implementation of Defensive Cyber Operations-Internal Defensive Measures (DCO-IDM) for rapid identification of new vulnerabilities, elimination of known vulnerabilities, and the fielding of new capabilities for defense-in-depth and incident response and analysis. DCO-IDM missions are conducted at the global and enterprise level and within DISA-operated portions of the DODIN to preserve its confidentiality, availability, and integrity.

• Improve mission assurance and critical infrastructure protection to reduce the risk to critical infrastructure and improve interagency and international partnerships. Support the Defense Industrial Base (DIB) program by enhancing the functionality and capacity of the unclassified and classified DIB Network to provide secure scalable, reliable, responsive, and collaborative information-sharing networks. The improved protection of assets enables the military advantage.

• Plan for the transition from peacetime to wartime operations by expanding exercise planning and participation to build proficiency, readiness, interoperability, and the mutual trust required for a joint approach to global campaigns. Produce annual contingency planning documents, including combatant command campaign plans, global campaign plans, and DOD top-priority contingency plans.

Strategic Goal 2 | Adopt, Buy, and Create Solutions

The Adopt, Buy, and Create Solutions process improves the speed of delivery of services and capabilities for the DOD. When a mission partner requests a solution, the agency implements the process to determine the best way to meet the requirement. First, the agency determines if the solution already exists within the DOD and if it is scalable to meet the mission requirement. Second, if the solution is not available or scalable, the agency buys it from industry partners. If the solution is not available from DOD or industry partners, the third - and least agile - method to fulfill the requirement is by creating a custom solution. When this is required, the agency provides short-term solutions to fill the capability gap, while the long-term solution is developed and implemented. This process strengthens mission partner collaboration by developing and delivering a customized service or capability solution based on their unique requirements.

Strategic Objective 2.1 | Optimize for the Enterprise

DISA optimizes enterprise services and capabilities to minimize costs and complexity while delivering a consistent user experience with high performance, availability, and reliability. The convergence and transition to these collaborative capabilities leverage current infrastructure and expands to cloud-enabled enterprise services. Enterprise solutions will enable an authorized user or device to access authorized data and services at any time, from anywhere.

• Leverage the benefits of cloud across all services and capabilities. Invest in commercial cloud capabilities and support the DOD cloud initiative to modernize the IT enterprise. Operate the primary commercially owned and operated service, providing our mission partners cloud-based resources dependent upon mission requirements.

• Provide unified capabilities to replace disparate legacy enterprise IT services for office productivity, messaging, content management, and collaboration. Deliver unified capabilities through multiple enterprise collaboration and productivity services capability sets that improve interoperability and enhance cybersecurity to achieve integrated and seamless communication DOD-wide.

• Deliver a modernized capability for the C2 portfolio to enable the right communications at the right time. The rapid evolution of digital technologies has introduced new challenges to the traditional command and control landscape. Modernizing the Global Command and Control System – Joint Enterprise, and Joint Planning and Execution Services portfolios mitigate vulnerabilities and risks.

• Establish internal processes and business re-investment strategies to modernize and streamline the execution of core functions. Implement Software Defined Enterprise (SDE) to integrate and connect the different automated services and business systems to facilitate all automation components within the architecture to communicate and provide closed-loop operations. SDE will lead to reduced operating costs, reduced service delivery time, improved standardization, performance and scalability, and faster response to cyber-attacks.

Strategic Objective 2.2 | Strengthen Cybersecurity

The current cyber domain is a dynamic, complex, and contested battlespace constantly under attack by an ever-evolving array of highly competent adversaries. These malicious actors seek to leverage the characteristics of the cyber domain to their advantage and compromise our ability to operate effectively in cyberspace. The cybersecurity environment is enhanced, standardized, and centralized to defend against evolving threats.

• Enhance the defensive architecture with a focus on defending against both external and internal attacks, detecting lateral movement, and fully incorporating more robust endpoint capabilities in a synchronized and standardized defensive implementation. This standardized and centralized security infrastructure supports active configuration management while also being resilient and agile enough to support passive and active mitigations.

• Implement AI and machine learning (ML) to support the cyber defenders in identifying malicious actors through the automated analysis of cyber sensors, threat indicators, and system outputs. As the AI/ML program matures, we are closer to systems fighting systems, reducing workhours invested. This consistent environment facilitates global shared workflow and integrated operations between global, regional, and mission partner commands.

Create

Strategic Objective 2.3 | Drive Innovation

DISA drives innovation to ensure the department remains competitive. We drive innovation by collaborating across the DOD to anticipate emerging mission partner requirements and then resource innovative solutions to meet the requirement. Innovation ensures that services and capabilities are provided to mission partners and JFHQ-DODIN at the speed of relevance. An innovative outlook, collaborative approach, and streamlined acquisition strategy improves customer service.

• Adopt a development, security, and operations (DevSecOps) culture and instantiate a DevSecOps environment and platform that supplies automated pipelines, tools, and standards needed to support the development of containerized applications at scale. Implement DevSecOps for rapid prototyping when buying or creating is the appropriate acquisition process. This combination facilitates accelerated innovation and delivery of enterprise IT services and capabilities.

• Implement acquisition strategies to drive innovation. Use the commercial solutions offering to speed up cloud-based internet isolation, assured identity, mobility enablement, and AI and ML platforms. Use the Other Transaction Authority to attract companies with leading-edge technologies. Once awarded, use the Systems Engineering, Technology, and Innovation contract to partner with small, innovative companies.

• Partner with DOD, industry, academia, and our allies to leverage private sector technical experts and research and development capabilities to rapidly innovate services and capabilities. These trusted partnerships are critical to bringing effective and secure capabilities to leaders and warfighters around the world.

Strategic Goal 3 | Enable People and Reform the Agency

DISA and JFHQ-DODIN's greatest asset is our people. Each day, all across the world, our people are motivated by a sense of duty that is inspired by service and accountability. We nurture a culture of continuous improvement by investing in education, training, and development opportunities for our workforce. Informed and engaged people are essential in recommending and implementing more effective systems and streamlined processes that lower overall workforce stress and administrative workload, and provide the maximum time available to focus on mission-related work.

Strategic Objective 3.1 | Enable People

DISA and JFHQ-DODIN foster a culture of trust and accountability to create a work environment that enables people. Trust and accountability are the foundation of a healthy work environment and essential to completing the agency's strategic goals and objectives. Achieving and maintaining a high level of trust is everyone's responsibility and positions the workforce to execute with strength, agility, endurance, resilience, and flexibility. Achieving and maintaining a high level of accountability ensures every employee and every mission partner has trust in DISA and JFHQ-DODIN.

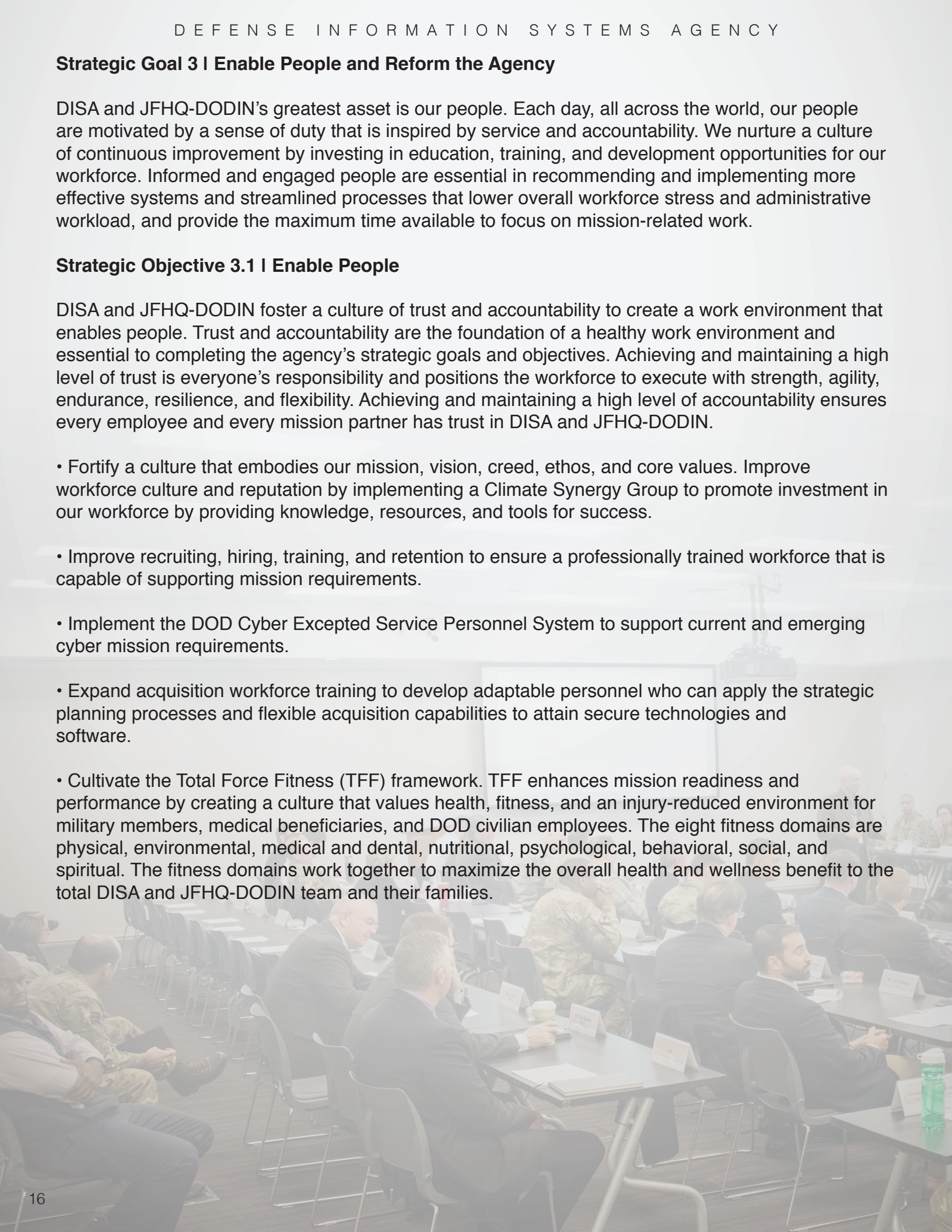
• Fortify a culture that embodies our mission, vision, creed, ethos, and core values. Improve workforce culture and reputation by implementing a Climate Synergy Group to promote investment in our workforce by providing knowledge, resources, and tools for success.

• Improve recruiting, hiring, training, and retention to ensure a professionally trained workforce that is capable of supporting mission requirements.

• Implement the DOD Cyber Excepted Service Personnel System to support current and emerging cyber mission requirements.

• Expand acquisition workforce training to develop adaptable personnel who can apply the strategic planning processes and flexible acquisition capabilities to attain secure technologies and software.

• Cultivate the Total Force Fitness (TFF) framework. TFF enhances mission readiness and performance by creating a culture that values health, fitness, and an injury-reduced environment for military members, medical beneficiaries, and DOD civilian employees. The eight fitness domains are physical, environmental, medical and dental, nutritional, psychological, behavioral, social, and spiritual. The fitness domains work together to maximize the overall health and wellness benefit to the total DISA and JFHQ-DODIN team and their families.



Strategic Objective 3.2 | Reform the Agency

DISA pursues reform and efficiency initiatives to increase performance and affordability for the DOD. We deliver on reform efforts through the DOD IT Reform Initiative and implement internal change that generates enduring value for our mission partners.

• Strengthen customer service by building an understanding of mission partner priorities through regular engagements and collaboration at all levels. Implement solutions to reduce the provisioning timeline.

• Contribute to the DOD IT reform effort to reduce costs and optimize enterprise IT capabilities by supporting network and data center optimization, automating continuous endpoint monitoring, streamlining IT commodity purchases, providing enterprise collaboration suites, and consolidating cyber / IT responsibilities.

• Attain and sustain an audit-ready status to demonstrate a commitment to financial excellence and stewardship of resources. Implement robotics and AI processes to improve and automate financial and contractual transactions.

• Rigorously test all services and capabilities before implementation and reduce duplicative testing efforts and overall programmatic costs by using the Joint Interoperability Test Command for all operation tests, evaluations, and assessments to deliver superior capability and cost savings to our mission partners.

Conclusion

DISA's strategic plan articulates our vision of a combat support agency that is the DOD's trusted provider to connect and protect the warfighter in cyberspace. It demonstrates our commitment to provide our mission partners with improved customer service in the delivery of their services and capabilities. It provides our workforce with the goals, objectives, and capabilities to build the strength, agility, endurance, resilience, and awareness to win in the cyberspace domain.

The strategic plan framework outlines mutually reinforcing programs, projects, and initiatives that link our three goals to the mission. To operate and defend, adopt, buy, and create solutions, and enable people and reform of the agency, ensures DISA conducts DODIN operations for the joint warfighter to enable lethality across all warfighting domains in defense of the nation.

The strategic plan is executed through the implementation of the framework and follow-on planning. Follow-on planning is conducted in each organization to determine the execution strategy. Collectively, the implementation of the framework and follow-on planning enable mission accomplishment.

References

- United States, and President Trump. National Cyber Strategy of the United States of America, The White House. September 2018
- United States, and President Trump. National Security Strategy of the United States of America, The White House. December 2017
- United States. Congress. Committee on Armed Services. National Defense Authorization Act for Fiscal Year 2019: John S. McCain National Defense Authorization Act, June 19, 2018
- Department of Defense, DoD Digital Modernization Strategy, Information Resource Management Strategic Plan FY 2019 – FY 2023, Version 0.5, January 15, 2019
- Department of Defense, Department of Defense Cloud Strategy, December 18, 2018
- Department of Defense, National Defense Business Operations Plan for FY 2018 – FY 2022, John H. Gibson II, Chief Management Officer, April 9, 2018
- Department of Defense, Secretary of Defense, Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, January 18, 2018
- Department of Defense, Summary Department of Defense Cyber Strategy, 2018
- Department of Defense Instruction, DODI 8010.01, Department of Defense Information Network Transport, September 10, 2018
- Department of Defense Directive, DODD 8140.01, Cyberspace Workforce Management, Incorporating Change 1, July 31, 2017)
- Department of Defense Directive, DODD 3000.06p, Combat Support Agencies (CSAs), July 8, 2016
- Department of Defense Directive, DODD 5105.19, Defense Information Systems Agency (DISA) Charter, July 25, 2006
- Chairman of the Joint Chiefs of Staff, National Military Strategy, 2018
- Chairman of the Joint Chiefs of Staff Instruction 6211.02D, Defense Information Systems Network Responsibilities, Directive, Current as of 4 August 2015
- Chairman of the Joint Chiefs of Staff Instruction 3500.01H, Joint Training Policy for the Armed Forces of the United States, April 25, 2014
- Chairman of the Joint Chiefs of Staff Guide 3401D, CRS CJCS Guide to the Chairman's Readiness System, November 25, 2013
- Chairman of the Joint Chiefs of Staff Instruction 3405.01, Chairman's Total Force Fitness Framework, September 1, 2011
- United States Cyber Command, Achieve and Maintain Cyberspace Superiority, April 2018
- United States Cyber Command, OPORD 8500-19, Annex J, para 3.A.D.5
- Defense Information Systems Agency (DISA), DISA DISN Technical Evolution Plan FY18-23, January 5, 2018
- Defense Information Systems Agency, Near Term DCO Strategy, December 17, 2018
- Joint Force Headquarters – Department of Defense Information Network (JFHQ-DODIN), JFHQ-DODIN Subordinate Campaign Plan 8600

/USDISA

www.disa.mil

@USDISA

This document supersedes the DISA Strategic Plan 2015-2020.