DEFENSE INFORMATION SYSTEMS AGENCY

STRATEGIC PLAN

FY2022–2024

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

LETTER FROM THE DIRECTOR

We face a great global power competition, a changing cyber landscape with increasing risks and threats from state and non-state actors that together create an imperative for DISA to accelerate our efforts to connect and protect the warfighter in cyberspace. This strategic plan focuses our efforts toward a **shared transparency of understanding** so that we can achieve the **velocity of action** needed to win. We are taking bold and decisive action to ensure that the information technology that supports our current and next-generation warfighters and weapons systems are protected from intrusion and attack while creating secure access to critical information — anytime, anywhere. We are leveraging advances in automation to deliver and modernize capability at speed, while unifying security and the end-user experience to achieve an optimized enterprise IT environment. Achieving our strategic vision requires consolidating and standardizing IT services, adopting proactive early-warning monitoring or sensing practices, automating responses, migrating legacy services and capabilities to cloud-based offerings, and developing mobile capabilities at all classification levels so that our support to the mission is never diminished, regardless of work location. None of these efforts are possible without the innovation, dedication and selfless service of our workforce. We are challenging them to achieve our goals and meet the needs of the Department quicker and with greater effectiveness. I am proud to say that DISA embraces these challenges, while becoming better at what we do every day. This strategic framework, along with the in-house action plans we create to operationalize these lines of effort, provide the clarity we need for success today and in the future.

Lt Gen Robert J. Skinner
United States Air Force
Director

PURPOSE

Articulate our mission and vision as the Nation's premiere IT combat support agency and the trusted provider to connect and protect the warfighter in cyberspace. We support the joint forces' ability to win against any adversary, adapt to unexpected changes and sustain any campaign, while maintaining readiness to address the next challenge. DISA provides, operates and assures command and control, information-sharing capabilities and a globally accessible enterprise information fabric that directly supports national-level leaders, the military services, combatant commands and coalition partners across the full spectrum, from competition through conflict.
Our agency's approach reinforces the lines of effort within DOD, strengthening the security and resilience of networks and systems that enable U.S. military advantages. This strategic plan is an overarching framework to explore technologies and evolve service delivery to drive a more secure, seamless and cost-effective DOD IT architecture. It serves as the foundation for our FY 2022-2024 internal action plans.

MISSION

To conduct Department of Defense Information Network (DODIN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation.

VISION

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

STRATEGIC OBJECTIVE

The current environment of great power competition requires our agency to deliver capability to the warfighter with a velocity of action to win. We must evolve our organizational design and operating processes to align with next generation capabilities, defend against new cyberspace threats and increase lethality for our warfighters while ensuring the best value.

LINES OF EFFORT (LOE)

The actions in support of our lines of effort will implement, sustain and evolve the global network infrastructure and unified capabilities to provide information superiority to the President, the Secretary of Defense, combatant commanders, senior leadership, military services, defense agencies and the warfighter. The challenges posed in the strategic objective are addressed through our lines of effort (LOE): prioritize command and control, drive force readiness through innovation, leverage data as a center of gravity, harmonize cybersecurity and the user experience and empower the workforce. Key focus areas throughout these LOEs include improving efficiency and effectiveness, reducing time to deliver solutions, cutting costs, standardizing services and implementing capability both internally and for our mission partners. New LOEs or actions may be added when necessary to support an agile approach and to achieve our shared vision.

PRIORITIZE
COMMAND AND CONTROL
DRIVE
FORCE READINESS THROUGH INNOVATION
LEVERAGE
DATA AS A CENTER OF GRAVITY
HARMONIZE
CYBERSECURITY AND THE USER EXPERIENCE
EMPOWER
THE WORKFORCE
VELOCITY OF ACTION TO WIN
DISA: TRUSTED TO CONNECT, PROTECT, AND SERVE

PRIORITIZE

LINE OF EFFORT #1: PRIORITIZE COMMAND AND CONTROL (C2)

Information is a critical C2 enabler for warfighters and mission partners. Our agency continues to address the capability and service needs of the warfighter through global mission partner engagement and information sharing. To achieve the Department's Joint All-Domain Command and Control (JADC2) vision, we will streamline C2. This, combined with our cyberspace operations and cybersecurity situational awareness unities of effort, enable warfighters to make mission-based, real time decisions at the tactical edge. Our work makes Presidential and senior leader communications, continuity of operations and government communications, and Nuclear Command, Control and Communications possible.

Modernization of warfighter support systems and unified capabilities improves C2, information sharing and decision support across the Defense Information Systems Network, a key component of the DODIN. We will continue to improve resiliency, capability and security in support of communications, while modernizing and sustaining senior leader communications with the latest cybersecurity capabilities. Furthermore, we will sustain our ongoing efforts to migrate Fourth Estate and other organizations to a consolidated network, DoDNet. By moving commonly used IT services to DISA, agencies can focus on their individual missions in support of the warfighter. DISA will also continue to focus on speed and transparency while providing a full range of DOD IT services to the Pentagon and National Capital Region:

- **Transport** — Modernize the DODIN backbone by leveraging software defined technologies, commercial innovations and multimedium avenues (i.e., space, terrestrial, etc.) to create a unified enterprise network for unclassified and classified communications; accelerate the speed of information access for our joint warfighters while reducing costs to mission partners.
- **Network Consolidation** — Consolidate, integrate and unify disparate and stovepipe networks into DoDNet.
- **Cyberspace Operations** — Deploy automation for proactive sensing of the C2 environment to drive incident avoidance, rapid response and increased operational agility.
- **National Leadership Command Capability** — Invest in delivering state of the art IT capability to our Nation's leaders by improving security, resiliency, flexibility and capacity of DOD networks; standardize configurations for greater performance, effectiveness and affordability.
- **Combatant Command Support** — Maximize effectiveness as a combat support agency with rapid response to warfighter requirements and expansion of common IT support to the endpoint.

LINE OF EFFORT #2: DRIVE FORCE READINESS THROUGH INNOVATION

We are driving implementation of next generation technology to ready DISA to address the future fight. We will integrate these capabilities while leveraging industry best practices to efficiently adopt secure, enterprise-class technologies to facilitate real-time, mission-enabling solutions across different platforms, devices and classification levels. Much of our success in this area comes through partnerships with industry and academia, and the use of innovative acquisition strategies.

We are implementing multiple contracting initiatives to ensure best value in all our programs. One of the programs, Joint Warfighting Cloud Capability (JWCC) seeks to create a multi-vendor acquisition vehicle that the greater DOD can leverage to obtain services directly from commercial cloud service providers. This would eliminate the need for third party resellers, integrators, achieving efficiencies as a result. The program acquires and implements common enterprise applications and services for joint use across DOD, standardizing cloud adoption and enabling cross-department collaboration. DISA will continue to deploy these office solutions using a multifaceted approach for classified and unclassified environments, facilitating migration from legacy enterprise services and sunsetting legacy services. We will explore and adopt synthetic-user monitoring capabilities to gain near real-time visibility of network and application performance and drive improved service delivery and remain postured to be the premier provider of hybrid-cloud solutions for our mission partners. We will continue to deliver:

- **Speed to Capability** — Maximize development, security, operations (DevSecOps) and agile development to reduce the time required to develop, secure, test and field IT capabilities and services to the warfighter.
- **Automation and Orchestration** — Expand use of automation and orchestration to enhance interoperability, speed of provisioning and performance monitoring; leverage robotic process automation (RPA) for increased efficiency, enabling DOD to reduce time to deliver, reduce operational costs and increase operational scalability.
- **Mobility** — Enable a mobile workforce; deliver modern secure IT solutions that facilitate delivery of DOD mission applications to the endpoint at all classification levels.
- **Cloud Adoption** — Transform traditional hosting capabilities and deliver streamlined alternatives to accelerate the Department’s adoption of cloud; deliver capability at all classification levels.
- **Emerging Technology** — Develop a technology roadmap to drive the evolution of current state architectures and services toward next generation capabilities; minimize labor-intensive and time-consuming processes by Artificial Intelligence / Machine Learning solutions to free our workforce to devote their time to higher-value work.

LEVERAGE

LINE OF EFFORT #3: LEVERAGE DATA AS A CENTER OF GRAVITY

As DOD embraces several data-management initiatives, we seek to build a culture that values data as a strategic asset to drive mission effectiveness. When thoughtfully collected and analyzed, data can accelerate innovation and improve service delivery. There is also an inherent power in owning data to control the high ground. DISA's chief data officer (CDO) will drive the agency toward a more data-centric culture and ensure that data is discoverable, accessible and decision-enabling through secure and modernized systems, standards and governance. The CDO will lead the development, integration and management of solutions to support data management, data security, advanced analytics and business intelligence to leverage data in day-to-day operations and decision making tools like Big Data Platform. Through the JADC2 program, we are working collaboratively across the federated mission partner environments (MPE) to enable visibility, access and integration of data. Leveraging cyber, business performance and analytical data encourages our total force and mission partners to accelerate innovation by exploiting untapped efficiencies:

- **Data as an Asset** — Invest in data as a strategic asset, using discovery, cataloging and analytics.
- **Data Architecture** — Build a cohesive data architecture that enables transparency and data sharing, and encourages data collaboration and sensing for cyber and business analytics.
- **Advanced Analytics** — Develop advanced analytics and business intelligence to enhance day-to-day decision-making and capabilities for joint all-domain and electromagnetic spectrum operations.
- **Cyber Situational Awareness** — Create an enterprise defensive cyber operations (DCO) and data monitoring strategy to optimize use of data as a strategic asset.
- **Data Culture** — Promote a data-centric culture within the workforce.

LINE OF EFFORT #4: HARMONIZE CYBERSECURITY AND THE USER EXPERIENCE

HARMONIZE

Our agency is on the leading edge of deploying, operating and sustaining cyber tools, capabilities and expertise to maximize DODIN operations. We are pursuing actions across the complete spectrum of domains, transport layers and technologies to enhance, standardize and centralize our threat-based defense of the cybersecurity environment. We are actively aligning our efforts with a zero-trust security and software defined network architecture model to eliminate the traditional approach to identity management that is based on trusted or untrusted networks, devices and user credentials. Successful deployment of this model will achieve the DOD's goals to integrate network and security solutions in the cloud and to enhance protections of end-user devices. We will invest in commercial cloud capabilities to build enterprise identity and authentication solutions for DOD cloud environments to make data accessible to every owner from anywhere at anytime.

The agency is exploring ways to operate in a secure information environment while creating an optimal user experience. As the lead IT service provider for DOD, the users experience is of the utmost importance. With a focus on customer advocacy, the agency is leveraging technology insertion through the DevSecOps / Agile software development framework, automation and machine learning to deliver services to our mission partners with added focus on ease-of-use, transparency, storefront upgrades and data-driven decision capability. Through all these efforts, we are enabling the integration of data to make foundational activities in artificial intelligence possible. We will continue to modernize business systems to support the priorities of the Department with rapid delivery and effective services and capabilities.

- **Zero Trust "Thunderdome"** — Create a new zero trust security and network architecture that is dynamic and adaptable, and can be extended from the user to the data edge; align endpoint modernization and Comply-to-Connect capabilities; unify duplicate and regional security services; and leverage secure access service edge (SASE) solutions to reduce the dependence and load on existing internet access points (IAPs).
- **Continuous Monitoring** — Incorporate DCO continuous monitoring into the accreditation process to move the Department to a continuous authorization to operate (ATO).
- **Accessibility** — Create a Gray Network (GIPRNet) to provide access to secure resources from any location; provide scalable endpoint capability via enterprise identity, credential and access management (ICAM).
- **End User Experience** — Deliver modernized IT solutions that enhance security protections and increase endpoint performance.
- **Containerized Solutions** — Leverage industry to increase development and adoption of containerized security solutions, increasing speed to capability and reducing ATO timelines.

EMPOWER

LINE OF EFFORT #5: EMPOWER THE WORKFORCE

We are a highly complex global organization, composed of military, civilian and government contractor personnel. We recognize the importance of empowering and cultivating an innovative and diverse workforce through a framework that assures accountability, transparency and integrity with military and civilian talent leading within every level of the organization. Diversity of talent is important at DISA because different perspectives enhance problem solving, innovation and service delivery. Our agency is focused on establishing a talent pipeline of high-caliber candidates to serve as the next generation cyber workforce. We will continue to offer professional, leadership and personal growth opportunities to fully develop and retain highly motivated and qualified employees across the agency in support of the warfighter. We recognize the positive impact that a well trained and equipped workforce has on organizational climate and morale and will focus considerable emphasis on developing the next generation of leaders throughout the agency.

- **Trust Culture** — Build a culture of trust, inclusion, diversity and transparency.
- **Highly Skilled Workforce** — Actively recruit, attract and retain high-caliber candidates to serve as the next generation workforce, delivering next generation capabilities for agency operations.
- **Empowering Excellence** — Empower the workforce at all levels to meet our agency's mission needs.
- **Institutional Silliness** — Ruthlessly identify and remove policies, technologies and artificial barriers that inhibit best value.

THE WAY FORWARD

The framework addressed through our LOEs — prioritize command and control, drive force readiness through innovation, leverage data as a center of gravity, harmonize cybersecurity and the user experience and empower the workforce — articulates our vision of a combat support agency that is the Nation's trusted provider to connect and protect the warfighter in cyberspace. We look forward to working with our mission partners, industry and academia as we continue to strengthen our capabilities and achieve ***velocity of action to win***. ■

DEFENSE INFORMATION SYSTEMS AGENCY

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA.mil

DEFENSE INFORMATION SYSTEMS AGENCY

STRATEGIC PLAN

FY2022–2024