# DISA Next
## STRATEGY
### FISCAL YEAR 2025 – 2029

To campaign,
    to respond well in crisis,
        to fight and win.
    To gain and maintain relative
    advantage in cyberspace;
to make the DOD better.

# Director's Forward

Great strategy is about alignment … time, people and money, under the rubric of change. As a combat support agency and the premier IT service provider for the Department of Defense, we will continue to provide world-class services. At the same time, we are changing. We are re-organizing, optimizing and transforming to deliver resilient, survivable and secure capabilities to enable department success and warfighter lethality.

Throughout its 63-year history, DISA has harnessed change as DOD leveraged the agency to solve enterprise-level problems. In 1960, DISA (known then as the Defense Communications Agency) was charged with consolidating disparate service networks into a common voice, secure voice and data network. Thirty-two years later, the DOD tasked DISA to consolidate 194 data centers and 122 associated networks into 16, optimizing the Defense Department. In 2024, the DOD continues charging DISA to solve enterprise-level, hard and complex DOD-wide IT and communications problems in a dynamic world.

The purpose of this strategy is to drive this combat support agency's priorities and initiatives to deliver capacity and capability to our warfighters.

This DISA Next strategy describes where the agency is headed over the next few years. There are a few key initiatives I want to call special attention to – specifically a few DOD-wide, enterprise-level solutions DISA must develop. Our first priority is to simplify the network with large-scale adoption of a common IT environment. Consolidating combatant commands and defense agencies and field activities into this environment is a whole-of-agency effort and a key first step in providing a DOD-wide warfighting information system.

Second, we must develop a fully functional DOD enterprise cloud environment. That means we must provide both an active and self-managed cloud space. We must enable secure cloud access and provide relevant tools DOD customers need to fully realize cloud capabilities.

Our third priority is to integrate our Identity, Credential and Access Management and Zero Trust capabilities with our common IT and cloud environment. Underpinning these is resilient and secure transport. Success is accomplishing these goals and staying aligned to the DISA Next strategy while simultaneously being prepared to react to the unforeseen.

I am confident the agency will succeed – we have no other choice. We are the combat support agency entrusted with connecting senior leaders and warfighters across the globe 24/7 – often during the most stressful and dangerous moments of their lives. We must continue to deliver while being challenged by great powers. From great power competition with the People's Republic of China, to supporting operations in emerging geographic areas of national strategic importance, both home and abroad.

Underpinning these capabilities is the heart of DISA, our people. We have an incredibly talented and critically thinking cohort of professionals, who have a clear picture of the future and outstanding support across the Defense Department. Velocity of action means speed and direction. Our workforce and leadership drive speed and our strategy provides direction.

*Robert J. Skinner*



*U.S. Air Force Lt. Gen. Robert J. Skinner is the director, Defense Information Systems Agency and the commander, Joint Force Headquarters – Department of Defense Information Network.*

*As the DISA director, Skinner manages a global network of more than 20,000 service members, civilians and contractors who provide defense communications solutions to the president, Department of Defense, secretary of defense, Joint Chiefs of Staff and combatant commanders. DISA operates joint, interoperable command and control capabilities for the department, which support more than 200,000 warfighters in 150 countries.*

*As the JFHQ-DODIN commander, Skinner drives unified action across the DOD to secure, operate and defend the DOD Information Network. He leads the establishment of DODIN priorities, directs threat-informed actions through formal planning and future operational initiatives and oversees the command and control of daily unified network operations, cyber security actions and defensive operations on the DODIN.*

# DISA Next and the National Defense Strategy

DISA is the combat support agency entrusted with the Defense Department's information system network. It is our responsibility to transform and integrate our capabilities and services to best support the DOD. The National Defense Strategy defines our priorities and guides this transformation process.

The 2022 NDS describes four priorities: defend the homeland, deter strategic attack, deter aggression and if deterrence fails, win and ensure our military advantage by building a resilient Joint Force and defense ecosystem. DISA supports all four priorities. We are designed and chartered to operate and secure critical warfighting information technology that enables the DOD to defend, deter, fight and win.

The fourth NDS priority, building a resilient Joint Force and defense ecosystem, clearly describes the transformation the agency must take. It outlines the need to maintain information and decision advantage, preserving the joint warfighting system while operating in an all-domain denied, degraded, intermittent and low-bandwidth environment. The NDS characterizes this resilient defense ecosystem as being "robust, autonomous, modern, hybrid, integrated and next generation." Maintaining our information advantage and preserving joint warfighting systems are the DOD Information Technology problems this strategy seeks to solve.

This strategy communicates what suite of capabilities and services we intend on delivering to transform the DOD information system to meet the challenges described in the NDS. DISA cannot solve this problem alone. We need Congress, the DOD, industry and academia unified towards this common purpose.

Communicating our strategy enables a more focused effort across the DOD and ensures that we have addressed the unique challenges of the CCMDs, their multitude of mission sets, their warfighting functions and account for any domain-specific equities. We seek to avoid unnecessary duplication of capabilities between the CCMDs, DAFAs and military departments. We must capitalize on opportunities to simplify the IT environment, experiment with emerging technologies and test our solutions in the environments in which the Joint and Coalition Forces operate. We seek to partner with industry and academia to shape IT innovation towards solving our information system challenges. Furthermore, we must foster transparency to Congress as we work to resource this strategy and ensure we are meeting the DOD's information system needs.

# DISA's Strategic Planning Framework & Strategic and Operational Imperatives

The strategic planning framework aligns agency day-to-day, 5-year and 5- to 10-year efforts to the NDS. At the heart are four strategic, six operational imperatives and eight goals – all crucial to DISA's core functions that guide DISA's support to the warfighter and mission partners.

The first two strategic imperatives and four operational imperatives describe DISA's day-to-day mission. As a combat support agency, DISA is designed and chartered to execute these critical functions. These imperatives align to NDS priorities one through three and reflect how DISA enables the Defense Department and Joint Force as they deter, defend and campaign.

Our 2030 goals are eight specific areas of transformation DISA is focused on over the next five-years aligned to NDS priority four, resilient Joint Force and Defense Ecosystem.

The third and fourth strategic imperatives and fifth and sixth operational imperatives describe a longer 5- to 10-year look at agency transformation aligned with NDS priority 4. These imperatives capture the elements of the DOD's desired information system that DISA is responsible for implementing – in the 2030-2035 timeframe.

## IMPERATIVES

A strategic imperative is an overarching, vitally important function DISA must perform. An operational imperative is a more specific function – or specific responsibility – the agency must do within that parent strategic imperative. Everything DISA does is not captured in the imperatives; they simply reflect the essential mission partner-focused functions DISA performs as a DOD combat support agency.

## Strategic Imperative #1: Operate and Secure the DISA Portion of the DOD Information Network

The Defense Department designates the DISA portion of the DODIN as DODIN Area of Operation DISA, which encompasses the Defense Information System Network, the DISN DODIN boundary, multi-modal gateways, the transport layer and DISA services including on-premises and cloud data storage, applications, application hosting and more. Operate refers to the 24/7 management of DISA's terrain; whereas secure refers to DISA's responsibility to protect DISA's terrain, data at rest and data in transit.

### OPERATIONAL IMPERATIVE #1.1: PROVIDE RELEVANT, MODERN ENTERPRISE AND BUSINESS TOOLS

DISA provides a collection of over 200 enterprise and business tools to CCMDs, MILDEPs and DAFAs. Each of these essential tools is relevant to our mission partners' needs. DISA must provide state of the art capabilities that will not only meet current requirements but will posture their customers to take advantage of emerging capabilities that provide competitive advantages in a contested environment.

### OPERATIONAL IMPERATIVE #1.2: PROVIDE RESILIENT AND REDUNDANT DEFENSE INFORMATION SYSTEM NETWORK BACKBONE

One of DISA's primary responsibilities is to provide the DISN transport (DISN backbone), supporting network traffic for the entire Department of Defense. To ensure there are no breaks in service and that all traffic arrives at its destination unimpeded, it is critically important that DISA build survivability into the DISN. Resilient refers to the hardening and security of DISN circuits, boundaries and gateways, with sufficient bandwidth capacity to withstand network congestion and path failures. Redundant refers to the web and/or mesh of alternative circuits or modes of transport to enable re-routing or failing over.

### OPERATIONAL IMPERATIVE #1.3: MANAGE THE AGENCY

DISA is committed to fulfilling all regulatory and statutory requirements, while simultaneously enabling the agency to carry out its core functions. DISA's administrative activities that are crucial in this endeavor include governance, facility management, human capital initiatives and internal processes.

## Strategic Imperative #2: Support Strategic Command, Control and Communications

DISA is key to supporting the development, provisioning and operation of strategic C3 resources and capabilities – the systems, capabilities, networks and processes that enable command and control and allow senior leaders to communicate securely across the globe. Examples include the Defense Red Switch Network, capabilities that enable electromagnetic spectrum access, support to secure mobile devices, secure voice and video and continuity of government capabilities.

### OPERATIONAL IMPERATIVE #2.1: OPERATIONALIZE THE CLOUD

DISA is transforming its current cloud – the delocalized storage and hosting of data, information and applications – to better meet the DOD's need for a hybrid cloud environment. DISA's cloud service will be operationalized, meaning the agency will provide a secure cloud environment so warfighters may access data at the breadth, width and speed of modern combat operations.

## Strategic Imperative #3: Optimize the Network

DISA must optimize the DODIN to make it more efficient, secure, accessible, cost-effective, easier to manage and more capable of adapting to environmental changes. Optimization is critical to DISA's ability to deliver on the DOD and Joint Force needs.

### OPERATIONAL IMPERATIVE #3.1: UNIFY THE NETWORK

The Department of Defense will benefit from consolidating CCMDs and DAFAs into a unified network environment. DISA's approach will enhance network management and operations while ensuring maximum security and a seamless user experience. Unifying the network can provide vital enterprise-level solutions, such as single tenancy, common services and consolidated cloud and lead to a more efficient and effective organization.

### OPERATIONAL IMPERATIVE #3.2: DIVEST TECHNICAL DEBT

DISA cannot meet its goals if the agency maintains substantial technical debt. Technical debt is obsolete, redundant or a less-than-ideal material solution that only solves part of the problem and is maintained when a better solution is unavailable, or a mission partner continues to use a suboptimal solution. Divesting tech debt means that we must cease operating these suboptimal solutions because they take critical resources from achieving the agency's goals.

## Strategic Imperative #4: Operationalize Data

Operationalizing data means proactively collecting, storing, correlating and interpreting data – to generate information and knowledge that enables warfighters to make relevant and timely decisions. These decisions maneuver the DOD's information system through a complex, hostile and dynamic threat environment at the speed of light. Maneuvering through the cyber domain is fundamentally about seizing, retaining and exploiting relative positional advantage – we cannot seize the advantage without useful data.

We achieve positional advantage in three ways. The first is culture, which includes cyber policy, regulations and laws. Useful data demonstrates when and what changes to policy, regulations, and laws are required to avoid ceding key terrain to our adversaries. The second is cyber conduct. A useful data schema helps enforce compliance, for example, password and patch compliance, authoritative registries on users and devices and authorities to operate on and through the DODIN. The third is our cyber capabilities – our set of tools that monitor the information system. Here, useful data helps decision makers posture cyber forces dynamically at points of need, re-route traffic around hostile activity and block/mitigate emerging threat vectors. To ensure the lethality and efficacy of our cyber forces, DISA must operationalize the incredible amount of data the DODIN generates.

# WE MUST

Campaign.

Respond well in crisis.

Fight and win.

Gain and maintain relative advantage in cyberspace.

Make the DoD better.

## OPERATE AND SECURE DAO DISA
PROVIDE RELEVANT MODERN ENTERPRISE & BUSINESS TOOLS
PROVIDE RESILIENT & REDUNDANT DISN BACKBONE
MANAGE THE AGENCY

## SUPPORT STRATEGIC C3
OPERATIONALIZE THE CLOUD

## OPTIMIZE THE NETWORK
UNIFY THE NETWORK
DIVEST TECH DEBT

## OPERATIONALIZE DATA

**DISA Next**
STRATEGY 2025 - 2029

# TO ACHIEVE

## THE NEXT GENERATION:

Defense Information System Network

Hybrid Cloud Environment

National Leadership Command Capability
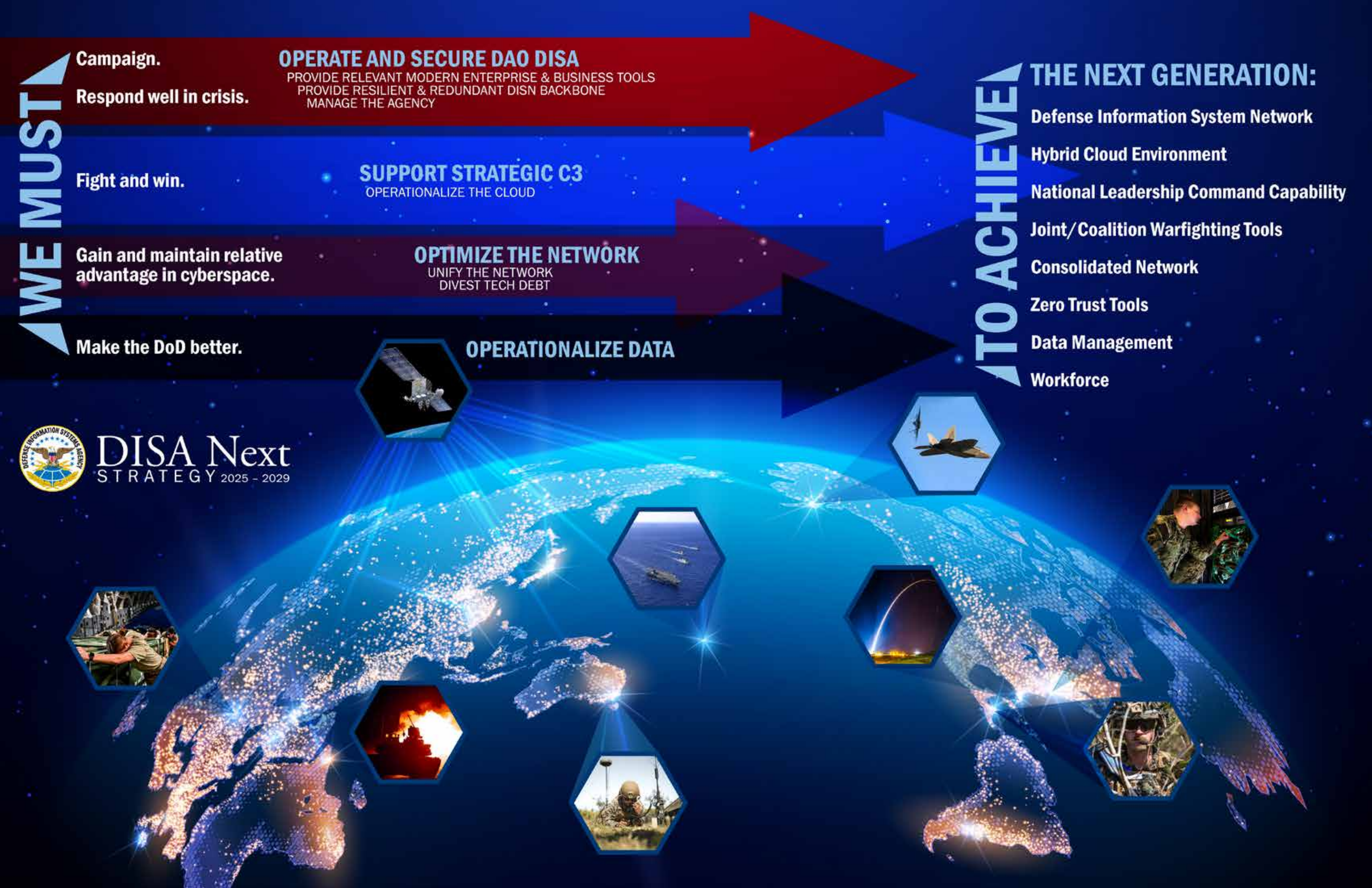
Joint/Coalition Warfighting Tools

Consolidated Network

Zero Trust Tools

Data Management

Workforce

GOAL 1

# The Defense Information System Network

*By 2030 DISA has a globally accessible, software defined, transport environment – unconstrained by bandwidth, impervious to denial, disruption, intermittent or limited access, that is seamless to the user.*

The warfighter requires constant connectivity and persistent access to mission-relevant data. A next-generation DISN provides this connectivity and access by transforming the transport layer, the boundary and the speed of delivery for DISA's services.

DISA transforms the transport layer by extending the DISN optimal transport system and by leveraging long-haul dark fiber, wavelength, leased bandwidth capacity and packet services at commercial facilities and available commercial ethernet, public internet and low latency non-geostationary orbit satellite transport services.

To fully realize this additional transport capacity, DISA will deploy software defined wide area network technologies, high-capacity routers and an underlying connectivity service.

DISA transforms the boundary with a new cloud access point architecture, new commercial ethernet gateways, optimizing internet access points and software defined edge gateways.

DISA transforms security at the boundary with media access control, improved cross domains security and ZT compliant capabilities. DISA increases the speed of delivery by exploiting advancements in automation technologies like robotic process automation and automated account provisioning.

In total, this next-generation DISN is a DDIL hardened, bandwidth-unconstrained, self-healing and secure fabric that provides warfighters constant connectivity and persistent access to their mission-relevant data.

> "The network that the Marine Corps needs […] must assure lethality and C2 in support of Joint and Naval operations globally […] to survive and win in contested domains from the enterprise through the tactical edge."
> — *United States Marine Corps Enterprise Network Modernization Plan*

> " By leveraging the cloud open-architecture, information can flow rapidly between the enterprise and Soldiers on the ground. This will enable commanders to counter adversaries in the information environment as effectively as they do in physical domains and win in the cognitive space."
> — *2019 Army Modernization Strategy: Investing in the Future*

GOAL 2

# Hybrid Cloud Environment

*By 2030 DISA is operating a resilient, globally accessible hybrid cloud environment rooted in DevSecOps principles and supports emerging "as code" and "as a service" capabilities.*

Consistent with the agency's DISN transformation, DISA must transform our current cloud services into the DOD's premier hybrid cloud environment, ensuring the warfighter's agile access to their data and applications.

DISA's hybrid cloud environment includes actively managed on-premises cloud, data centers, hosting capabilities and cloud-based tools. DISA's Joint Warfighting Cloud Capability 2.0 initiative is a multi-vendor, enterprise-wide acquisition vehicle that provides the DOD with a mechanism to acquire commercial cloud services directly from commercial cloud service providers.

To best support the Joint Force's global presence, DISA is revolutionizing the Joint Operational Edge program. JOE is an interconnected and integrated mesh of commercial edge computing platforms, installed at DOD locations, that delivers commercial cloud service offerings and necessary DOD enterprise common services.

DISA's hybrid cloud environment transformation also ensures the cloud boundary is secure with enhanced network monitoring and modern cloud access points, enabling information sharing to the tactical edge. This approach to securing our cloud boundary safeguards our information by utilizing the latest cybersecurity technologies and methodologies, denying our information to our adversaries, which helps to defend our warfighters around the globe.

GOAL 3

# National Leadership Command Capabilities

*By 2030 DISA has modernized DISA's portion of the NLCC fabric to enable national leadership and strategic coordination between allies and partners.*

DISA's portion of the NLCC fabric includes the DISN transport layer, secure voice, video and conferencing capabilities, support to secure mobile devices, critical time dissemination and support to the cloud. To transform our NLCC segment into a defendable sector, DISA must develop an approach to fund and implement zero-trust architectural guidance to ensure our end users can perform critical missions in a DDIL environment. DISA must implement a cryptographic modernization strategy that addresses areas requiring advanced crypto capabilities within the NLCC fabric.

Operating DISA's key NLCC capabilities is another no-fail, global, 24/7 DISA core function. The agency must work to fully understand DOD's requirements, rapidly prototype, test and deploy next-generation NLCC capabilities and maintain the world-class services DISA offers today.

> " To serve as the bedrock of integrated deterrence, ... we will need to continue partnering with industry to ensure flexibility, responsiveness and capacity."
> — *U.S. Army Gen. Anthony J. Cotton, commander, U.S. Strateigic Command*

GOAL 4

# Joint and Coalition Warfighting Tools

*By 2030 DISA has delivered the right suite of capabilities required to enable joint and coalition warfighting and has produced data standards that enable interoperability of approved joint warfighting IT solutions.*

DISA must develop and field the systems DOD needs to execute concepts like Combined Joint All Domain Command and Control, Joint Cyber Command and Control, Joint Fires Network and Joint Cyber Warfighting Architecture. The agency's role in this has three parts.

First, our DISN transformation is focused on DISA connecting the Joint Force and the ever-increasing military internet of things, from anywhere-to-anywhere, twenty-four hours a day, seven days a week. This includes the data layer where DISA's evolving hybrid cloud environment provides access and secures data at rest while the DISN protects data in transport.

Second, the DOD Chief Digital and Artificial Intelligence Office owns the DOD's data strategy and data layer. DISA however, plays a critical role in implementing those standards and deploying the suite of capabilities and services the DOD needs to realize a robust and useful warfighting data layer.

Third, DISA plays a critical role in enabling the Joint Force's use of the electromagnetic spectrum. It must develop the tools the force needs to control, manage. deconflict and make decisions about electromagnetic spectrum operations.

Modern warfare occurs in all domains — land, sea, air, space and cyberspace — and by, with and through coalitions. The U.S. Air Force is the executive agent for Mission Partner Environment. DISA, in close coordination with the U.S. Air Force, is uniquely postured to provide the mission partner environment the DOD needs to execute CJADC2 in a coalition environment. This includes cross-domain solutions between allied networks at all classifications levels, hybrid MPE cloud environments for planning and collaboration and a federated identity and a credential and access management system that enables coalitions to use shared command and control solutions.

> "Effective deterrence of threats in the Indo-Pacific requires significant investment to defend the homeland, protect the joint force, operate in contested space and provide all-domain battlespace awareness with integrated fires enabled by a joint fires network."
>
> *— U.S. Navy Adm. John C. Aquilino, commander, U.S. Indo-Pacific Command*

GOAL 5

# Consolidated Network

*By 2030 DISA has consolidated DAFAs and CCMDs into a common IT environment. This environment will offer seamless access to information at all classification levels and is postured to replace mission partner environments.*

Consolidating CCMDs and DAFAs onto a common network allows the DOD to eliminate numerous disparate networks, significantly enhancing operational efficiency. Consolidating enables DISA to oversee a unified, streamlined network, enhancing network agility, consistency and user support. Consolidation fosters interoperability and standardization, facilitating the deployment of capabilities such as software defined wide area networks and mobility devices. Streamlining the network bolsters security efforts by simplifying the terrain and allowing the agency to concentrate on cybersecurity defense assets and tools.

Consolidating CCMDs and DAFAs, along with MILDEPs or coalitions as necessary, represents a substantial undertaking for DISA. The agency must migrate multiple organizations at the same time while also conducting discovery and preparations for subsequent phases. There is an implied necessity for DISA to possess the essential infrastructure and trained workforce capable of supporting, managing and providing user support during the migrations.

> " Simplify, simplify, *simplify*. We need to simplify our processes, we need to simplify the infrastructure, we need to simplify the configurations and we need to simplify *how we do business with each other.*"
> — *U.S. Air Force Lt. Gen. Robert J. Skinner, DISA director*

## GOAL 6
# Zero Trust Tools

*By the fourth quarter of fiscal year 2027 DISA's portion of the DODIN complies with the ZT reference architecture and DISA is enabling DOD readiness through cost-effective ZT service offerings. Looking ahead to 2030, DISA aims to empower mission partner ZT solutions and data sharing environments.*

Defending the DISN with sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our data. Our current architecture spans global boundaries, interfaces with mission and industry partners and supports millions of authorized DOD users, many of whom access the DISN through virtual private networks at home or on their mobile devices.

DISA realizes ZT at the endpoint with comply-to-connect and telemetry-based access tools. At the mid-tier, DISA has developed and is fielding software-defined wide area networks and dynamic and flexible networking. At the perimeter, DISA has a secure access service edge tool and other capabilities that enable standardized access to DODIN resources.

Warfighting concepts like CJADC2, DOD's ever-increasing reliance on secure mobile communications and many of the emerging security requirements of the next generation DISN all require a single federated DOD identity, credentials and access management solution. In fact, enterprise ICAM provides a baseline capability to achieve a ZT architecture.

These capabilities, and end-to-end visibility, monitoring, automation, public key infrastructure, data tagging and ICAM constitute DISA's holistic approach to a ZT architecture that increases the DISN's resiliency and readiness posture against cyber threat actors.

> "We are determined to get zero trust across the department by 2027. It is a key priority for us, and we are firmly on that vector."
> *– Hon. John Sherman, DOD Chief Information Officer*

GOAL 7

# Data Management

*By 2030 DISA has a modern data platform for its defensive cyber and network operations data, has implemented standards for data management with relevant analytical tools tuned for DISA Defensive Cyber Operations/DODIN Operations; and integrated with other DOD data lakes.*
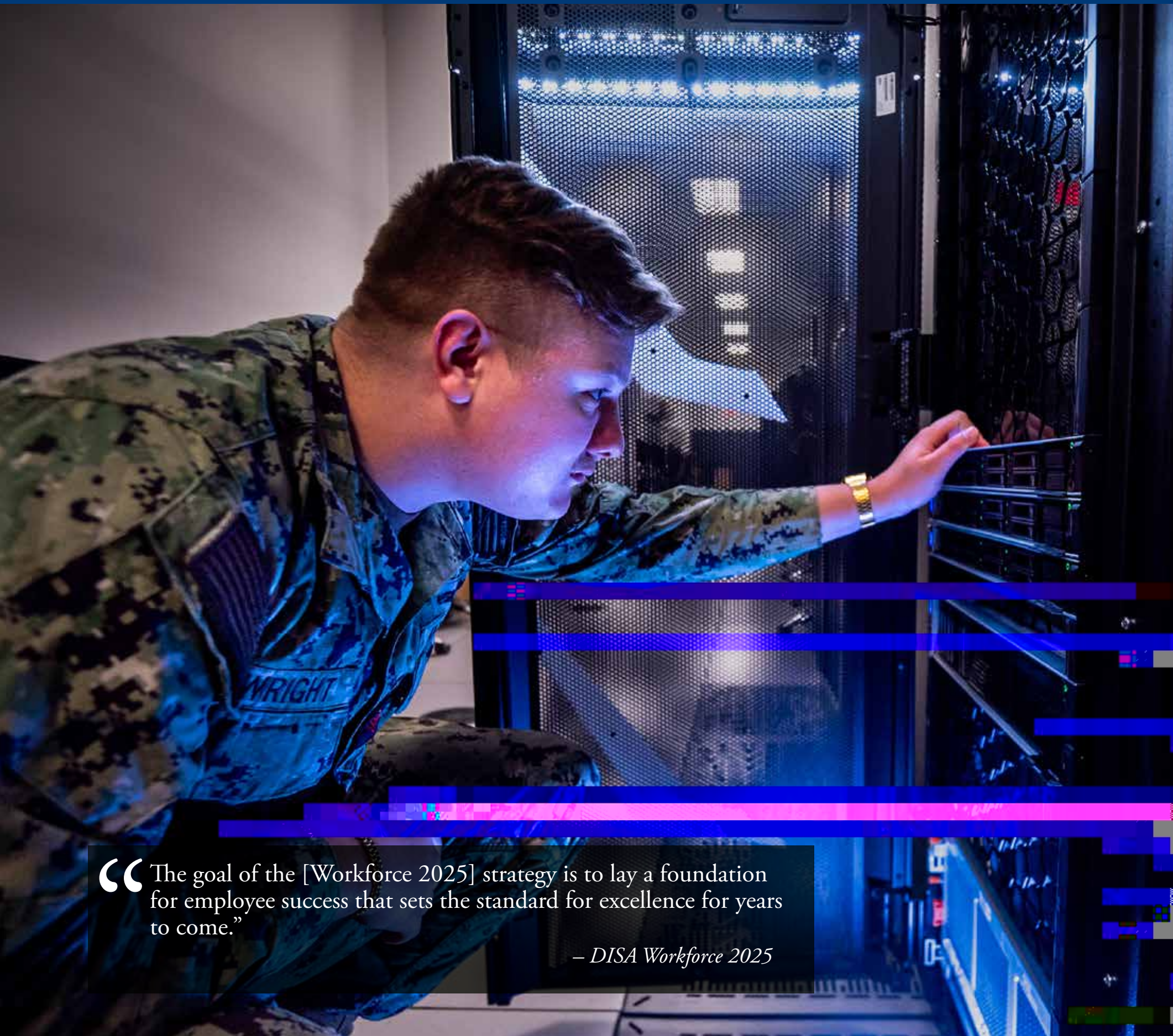
DISA's ability to make defensive cyber data useful is critical to our responsibility to secure the DISN. To do that we must first establish a data infrastructure that is integrated and scalable. This includes implementing both an agency and DOD Defensive Cyber Operations/DODIN operations data tagging schema, data catalogue, authoritative data sources, a big data platform, the right analytical tools to convert data into information and knowledge and good data governance.



" Deliver timely and trusted data at all levels to generate insights for more informed decisions."

*— U.S. Coast Guard Strategy*

> " The goal of the [Workforce 2025] strategy is to lay a foundation for employee success that sets the standard for excellence for years to come."
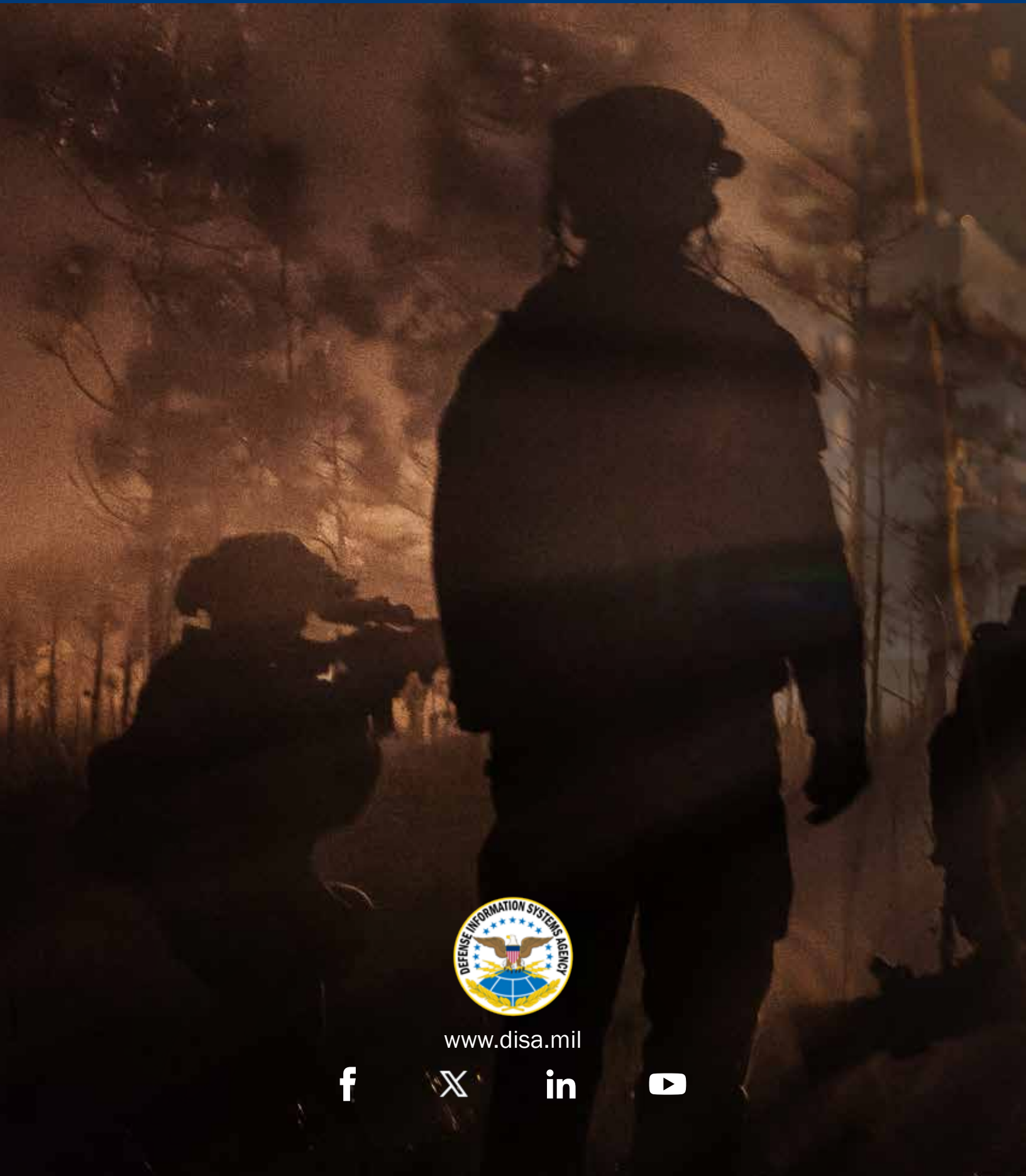>
> *– DISA Workforce 2025*

# Workforce

*By 2030 DISA will continue to upskill its workforce to remain lethal in today's IT environment; this workforce is empowered to excel and is optimally organized to meet the DOD's needs.*

DISA will only accomplish our goals by, with and through the efforts of a talented, trained and certified workforce. DISA must adopt a holistic and comprehensive personnel management approach designed to enhance the skills of our current employees while ensuring DISA onboards new talent and invests in the professional development of both throughout their careers. This includes a robust pipeline to bring talented college graduates, high-performing individuals from industry, other agencies and organizations, or military veterans with years of experience in the field, into the DISA workforce.

Operating in the cyberspace domain, requires a culture of continuous learning and skill development. Providing training and certifications is critical to our ability to attract and retain talent. To that end, the agency needs to leverage exchanges, rotations and educational opportunities that invest in individuals – a benefit to DISA long-term. DISA is also a learning organization that must continue to promote innovation at all levels. The best ideas don't always come from the top – developing talent empowers individuals and teams, leading to agile innovation.

*For the warfighter . . .*

*By, with and through allies and partners*
*Arm-in-arm with industry*

www.disa.mil