WINTER2023

DEFENSE INFORMATION SYSTEMS AGENCY

LOOKBOOK

DELIVER, OPERATE AND DEFEND

TABLE OF CONTENTS

DELIVER, OPERATE AND DEFEND

DISA FIELD COMMANDS/FIELD OFFICES

LOOKBOOK WINTER EDITION 2023

DISA Office of Strategic Communication and Public Affairs

TAMIKA JOHNSON	Project Lead	**ERIN WOLF**	Designer
DEVON SUITS	Editor	**T.L. BURTON**	Photographer

The Look Book is a publication produced by the Defense Information Systems Agency's Office of Strategic Communication and Public Affairs. It offers an in-depth look at a specific, select number of DISA's programmatic areas, in the words of personnel who are responsible for executing them. For more information, visit us at www.disa.mil, or contact us a disa.meade.bd.mbx.public-affairs@mail.mil.

DISN CORE

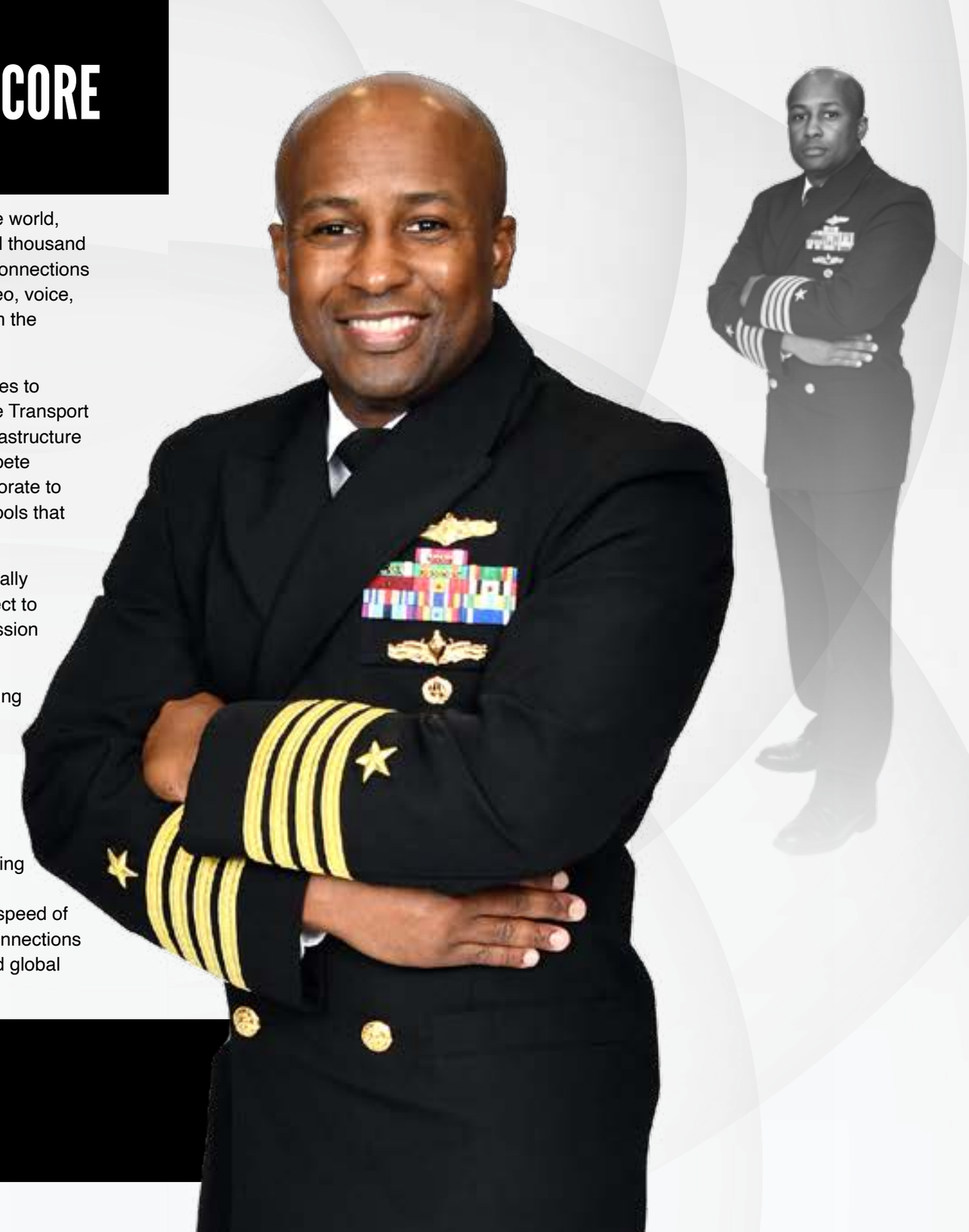
The Defense Information Systems Network, or DISN, is one of the largest networks in the world, spanning more than 100,000 miles of terrestrial and submarine fiber-optic cables, several thousand leased circuits and 355 delivery nodes. These delivery nodes serve as on and off-ramp connections to and from the DISN superhighway, enabling the Department of Defense to transmit video, voice, and data around the globe. Every day, DOD military, civilians and contractors benefit from the network services provided by the DISN.

For decades, DISA has worked to consolidate and integrate core DOD information services to reduce costs and bring the department's enterprise IT into a single ecosystem. Today, the Transport Services Directorate is collaborating with the military services to modernize the DISN infrastructure and provide the warfighter with optimized capabilities to meet the user demand and compete within an increasingly contested environment. Technological advances allowed the directorate to begin leveraging software-defined networking, next-generation transport and optimized tools that subsequently strengthen DISN resiliency, integrity and availability.

A further extension to the DISN infrastructure involves DOD teleport sites, which are globally distributed satellite communication facilities. Teleport sites enable satellite users to connect to the DISN long-haul networks and other internet-working functions ne cessary to meet mission requirements.

Transport Services Directorate technical experts are currently developing and implementing the Teleport Generation 3 Phase 3 capability to provide interconnectivity between legacy ultra-high frequency radios and the more recent Mobile User Objective System radios. To achieve the G3P3 capability, the program manager added two new components to the teleport architecture: the MUOS to Legacy Gateway Component and MUOS Voice Gateway.

The Transport Services Directorate is excited about the future. We are actively championing transport agnostic, cloud-centric, and DISN Forward concepts that aim to provide the warfighter with the most state of the art global network, regardless of location and at the speed of relevance. These forward-leaning concepts allow for an adaptive network and satellite connections capabilities to support primary, alternate, and contingency options, enabling uninterrupted global data exchange to the end user onboard a ship or on the battlefield.



U.S. NAVY CAPT. CHRIS GOODSON
Deputy Director
Transport Services Directorate

GATEWAYS

The Satellite Communications Gateway Program extends the Defense Information Systems Network and Department of Defense Information Network transport services to the warfighter via systems located at SATCOM gateways worldwide. Services are available to warfighters operating anywhere in the world over any band – wideband military and commercial, narrowband, and protected extremely high frequency bands.

SATCOM services involve stakeholders across all services, combatant commands and multiple agencies. By converging the Standardized Tactical Entry Point, or STEP, teleport and tools programs into a single portfolio the team will maximize and optimize infrastructure in keeping with National Defense Strategy and Space Warfare Analysis Center force design as the department builds toward Joint All-Domain Command and Control.

STEP and teleport convergence will provide users with a single baseline, along with a converged global mesh architecture and larger capability resource pools. Convergence also allows for more efficient mission planning and operational oversight. Technology refresh activities will improve the cybersecurity posture of DISA SATCOM gateway systems.

Our innovations are focused on becoming more efficient with the resources we have. We're doing this through partnerships with other parts of DISA and with our mission partners to realign, and in some cases, relocate the overall footprint of equipment we have to meet the global mission.

Looking ahead, the program expects to have a significant role in capability development for the Modernized Teleport System. The MTS will incorporate technologies that improve the overall capability and resiliency of the architecture, such as digital intermediate frequency, digital modems, routers with virtual device context capability and smart network planning tools that reduce planning and response times from weeks to minutes.

DAVID D. COMBS
Program Manager
DISA Satellite Communications Gateways

TELEPORT

In May 2000, the assistant secretary of defense for command, control, communications and intelligence designated DISA as an executive agent with the responsibility to design, develop, acquire and field DOD teleports to satisfy requirements approved by the Joint Requirements Oversight Council and detailed in operational requirements documents.

DISA established the DOD Teleport Program Office to carry out these responsibilities by way of upgrades to existing telecommunications capabilities and distribution points, which provide deployed forces with sufficient interfaces for multi-band and multimedia connectivity from deployed locations anywhere in the world to online Defense Information Systems Network service delivery nodes and legacy tactical command and control systems.

We are constantly looking at ways to improve performance by evaluating emerging and mature technologies that we can incorporate into the current capability to gain efficiencies, reduce footprint and virtualize where it makes sense.

Because of the critical importance of SATCOM to command and control and the ever-increasing threat, the team is currently looking at software defined networking, or SDN. While traditional networking is hardware-based, SDN is much more flexible than traditional networking as it allows administrators to control the network, change configuration settings, provision resources and increase network capacity all from a centralized user interface resulting in increased control with greater speed and flexibility, customizable network infrastructure and robust security.

The team's challenge on the horizon is implementing Office of Management and Budget Memo M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." Zero trust is the term for an evolving set of cybersecurity standards that move defenses from static, network-based perimeters to focus on users, assets and resources by shifting toward a never trust, always verify approach. The team is currently assessing assumptions, risks and implementation considerations of transitioning systems to zero trust.

The vision is retaining an acquisition program to deliver the next generation of SATCOM capabilities to meet an ever-increasing demand for bandwidth, capacity and coverage that will support the warfighter whenever and wherever the mission calls.

BRETT WAGNER
DOD Teleport Program Manager

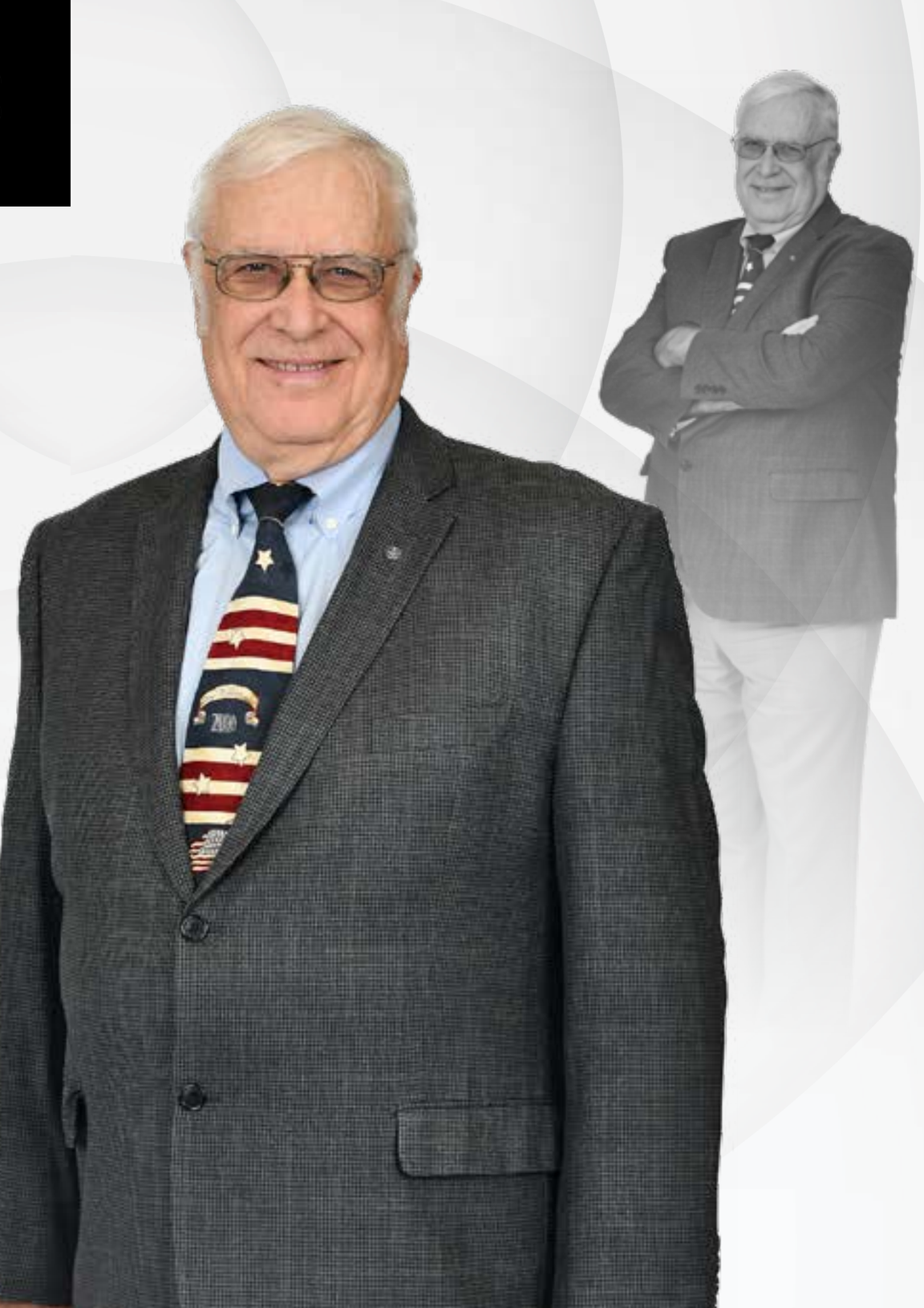
GLOBAL PUBLIC SAFETY COMMUNICATIONS NEXT GENERATION 9-1-1

DOD Directive 8422.01e, DOD Public Safety Communications Capability assigned the DISA director with the roles, responsibilities and authorities for the implementation of enterprise DOD public safety communications information technology architecture. The Director has established the DISA Office of Public Safety Communications Ecosystem Modernization in response to this tasking.

Public safety communications is a complex system of systems which include but are not limited to: next generation 9-1-1 call handling, computer aided dispatch, recording, text-to-911, dispatchable location, land mobile radio, First Responder Network Authority or FirstNetapps on government mobile devices, alarm and sensors, the internet of things, 5G, and enterprise mass warning and notification. As the implementation of public safety communications ecosystem modernization roadmap is designed and built, DISA will be able to ensure the first responders are able to communicate accurately, respond immediately and save more lives. This architecture will also apply to providing a more effective and immediate response to individuals experiencing a mental health crisis.

The team is constantly evaluating and putting new technologies into pilot programs to determine how these emerging capabilities will interact with legacy systems. Part of our philosophy is to partner with other federal agencies. Interoperability with mission partner systems is a critical element of the public safety communicators ecosystem modernization effort. Since our DOD Mission Partners retain title 10 authority to purchase equipment and services related to public safety, it is imperative that DISA ensure the architecture we develop is the best possible solution to meet the unique needs of our partners despite the varied mission requirements.

For the next two to three years, we're working on installing technology that will convert internet protocol data to analog data as a band aid approach. This is being done at DOD installations which are in states that are moving ahead with their modernization faster than we are. In the long term we're looking at fiscal year 2025 to start the real modernization effort and have it run for about five years across the Future Years Defense Program. Understanding and expecting the technology will continue to evolve and get better; however, our architecture is flexible enough to accommodate the new technology.



JOHN HOLLOWAY
Director
Office of Global Public Safety Communications

SPECIAL ACCESS PROGRAMS – INFORMATION TECHNOLOGY

The Compartmentalized Enterprise Services Office provides connectivity within the SAP-IT environment that enables executive leaders and mission partners throughout the Department of Defense and intelligence community to communicate within a powerful and secure enterprise environment that operates around the globe.

Our work aligns across all lines of effort within the DISA Strategic Plan. Through efforts to support SAP customers we prioritize command and control with mission partners by investing in and ensuring delivery of state-of-the-art IT capabilities to improve security, resiliency, scalability and capacity for our internal networks and applications. In addition, CESO seeks to continuously harmonize cybersecurity and the user experience through continuous monitoring and delivery of tools that enable a secure yet robust environment.

CESO is envisioning a new way to operate in a secured global environment while expanding our capabilities to include more of our defense partners. We are working with trusted partners to modernize legacy systems and applications and improve information sharing. The CESO team accomplishes this by ensuring we receive customer requirements before developing the roadmap and strategic plan for the program's information technology future. This allows DISA to provide stronger communication pathways, infrastructure stability, risk management, and customer relationship management.

In the immediate future CESO is working to reduce single points of failure by creating additional redundancy within the system. The CESO team will be migrating customers onto a new infrastructure to reduce lag time and improve the overall user experience. In addition, the focus will continue to be the development and strategy of the SAP-IT architecture to modernize the environment and be the premier provider of secure and flexible SAP-IT collaboration tools.

LINDA VANBEMMEL
Chief
Compartmented Enterprise Services Office

FOURTH ESTATE NETWORK OPTIMIZATION

Fourth Estate Network Optimization, or 4ENO, works by consolidating and standardizing information technology services with modernized and secure capabilities that supports our workforce, as well as current and next generation warfighters and weapons systems anytime and anywhere.

We're optimizing network capabilities by improving cybersecurity and IT support services for end users, while reducing operating costs by consolidating, integrating, unifying disparate and stovepipe networks into Department of Defense network. in support of DISA's strategic line of effort, "Prioritizing Command and Control." 4ENO is also delivering modernized IT solutions that enhance security protections and increase endpoint performance in support of harmonizing cybersecurity and the user experience.

As a first step, 4ENO is converging defense agencies and field activities, also known as DAFAs, networks and IT service help desks under DISA, as the single service provider. This will improve visibility of cybersecurity vulnerabilities, reduce operating expenses, and ultimately establish a common, optimal user experience. Network optimization for DAFAs will enable them to focus on their respective core mission, giving the single service provider role to DISA whose primary mission is the fulcrum for this unifying effort.

During the COVID-19 pandemic, our team overcame a heavy task never achieved before at DISA, by re-imaging laptops remotely rather than the typical on-site migration process. We've adapted DOD network to support a teleworking workforce; even our internal organization works from home.

We're empowering users regardless of what device they have, or where their work location is, on any given day. We want to create an environment of trust that their mission work is being done safely and securely. We're putting more emphasis on human centered design thinking and user experience concepts with each new technology insertion. We are working toward intelligent, automated processes that are highly adaptive and cyber resilient with scalable, cost optimized solutions that support a mobile workforce and mission needs. 4ENO is looking forward to working with other DOD agencies on their upcoming migrations to the DOD network.

LAURA HERBERTSON
Program Manager, Fourth Estate Network Optimization
Chief, Endpoint Services and Customer Support Division

GLOBAL SERVICE DESK

The Global Service Desk initiative began in 2015 with the goal of collapsing 108 disparate service desks and unifying them under common toolsets and simplify the “who do I call” for DISA’s customer base. After the realignment of service desk functions into one single organization, GSD assembled a team across the various service desk stakeholders to standardize operations and drive towards repeatable outcomes.

Over the last two years, GSD has Desk onboarded the Defense Finance Accounting Service Commodity and Mission Service Desk; Defense Technical Information Center, Defense Prisoner of War/Missing in Action Accounting Agency, and Defense Manpower Data Center Commodities under GSD’s Service Desk as a Service; and the Defense Logistics Agency’s Commodity as well as Mission Service Desk. Most recently, GSD assumed responsibility over the top secret service desks across the agency to provide upward mobility to service desk personnel and surge capability to ensure mission success GSD handled 1,673,932 customer interactions from August 2021 to July 2022. That is an average of 139,494 interactions per month.

The Global Service Desk Management Office serves as the single service support touch point for DOD customers utilizing DISA services and capabilities, DISA-hosted mission partner applications and DOD network’s commodity service 4th Estate Network Optimization initiatives for defense agencies and field activities.

We also offer two service offerings to the DOD: Service Desk as a Service to the DOD, which includes Tier I service support services via a live representative and Tier 0 self-help capabilities; and Automated Contact Distribution as a Service, which provides contact handling services to DOD customers for contact centers and service desks.

The GSD Management Office continues to work on an enterprise foundation data model data structure for the DOD, which enables our mission partners to escalate incidents and requests machine to machine. This will decrease ticket handle times by DISA and our mission partners, as well as enable both ticketing systems to be kept up to date in near real time.

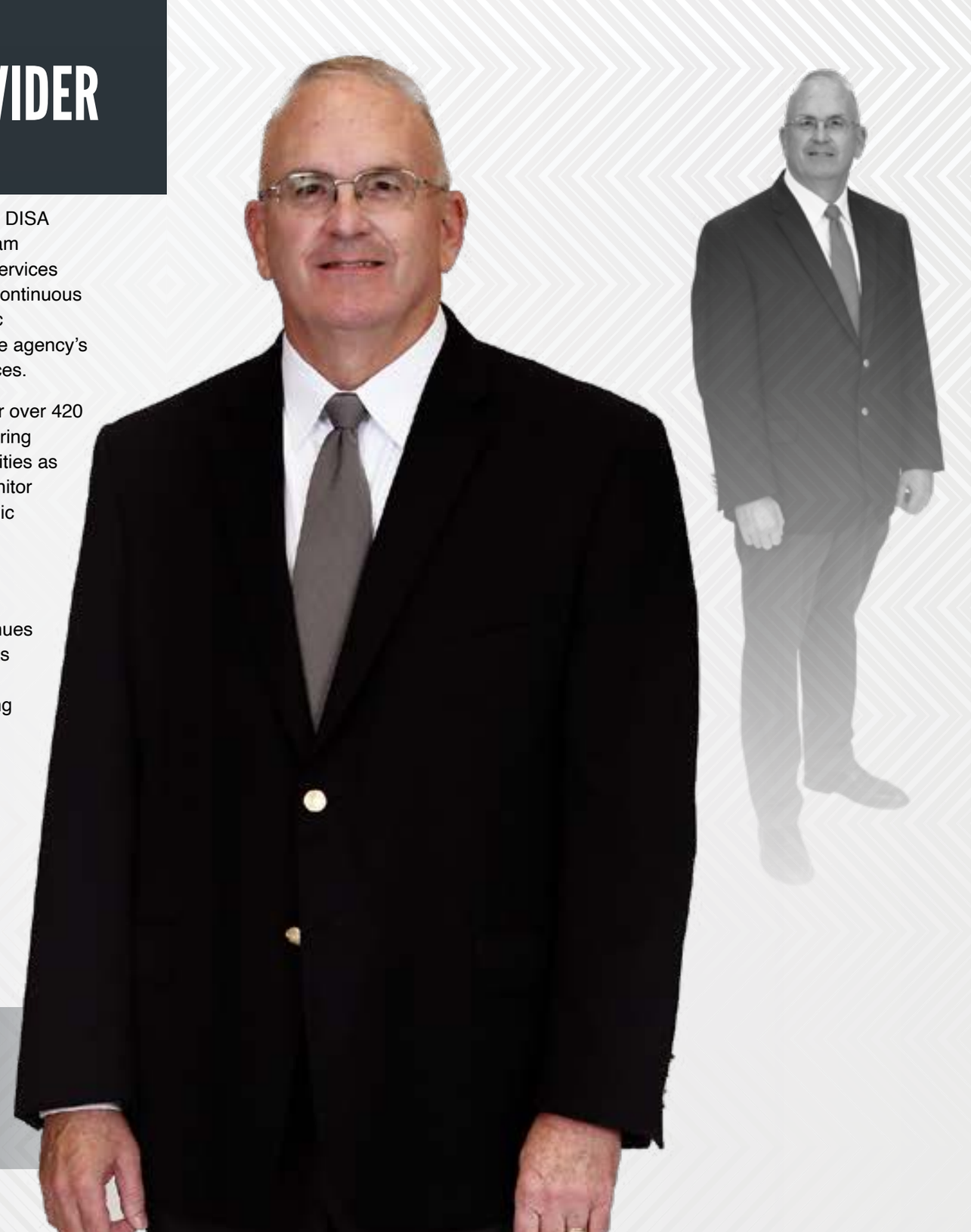
RICHARD FORSHT
Chief
Global Service Desk Management Office

CYBERSECURITY SERVICE PROVIDER

The Cybersecurity Service Provider Program Management Office delivers services to the DISA enterprise, combatant commands, Department of Defense agencies, and provides program oversight for services delivered to DISA's internal and external mission partners. These services include program portfolio management, customer management, service operations and continuous service innovation. As a program management office, we also engage in agency strategic development activities to assess the evolution of service effectiveness and to maintain the agency's authorization from Joint Force Headquarters-DOD Information Networks to provide services.

In the office, there are approximately 220 analysts that monitor just under 400 sensors for over 420 mission partners distributed around the globe. Our analysts defend the DODIN by monitoring network activities, maintaining cyber situational awareness and responding to cyber activities as a component of DOD's integrated cyber defense. In defense of the network, analysts monitor subscriber boundary, theater and global threat detection capabilities and leverage strategic end-to-end analysis to provide cyber security recommendations.

The program management office is made up of several integrated teams. The Portfolio Management Team manages the CSSP service portfolio, program funding, budget submissions and CSSP service catalog. The Transformation and Innovation Group continues to improve DISA's cyber defense capabilities for the agency and its customers and acts as operational subject matter experts guiding and advocating for innovative transformational capabilities. Our Customer Management Team actively manages the customer onboarding process to include documentation intake, service package creation, quote generation, service implementation and ongoing customer outreach. The Strategic Initiatives Team reviews and assesses DOD, federal, and commercial cybersecurity policies, directives, guidelines, DOD initiatives and governance processes to ensure the agency CSSP team is meeting all regulatory requirements. The Service Operations Management Team provides broad support to the DISA CSSP operations enabling effective execution of CSSP services. The team manages the CSSP inspection readiness to ensure the program retains its accreditation as an authorized DOD cybersecurity service provider.



DARRELL FOUNTAIN
Chief
Cybersecurity Service Provider Services

DEFENSIVE CYBER OPERATIONS

The Defensive Cyber Operations Division is part of the DISA Joint Operations Center, or DJOC, and directly supports the DISA strategic plan in our charge to defend the Department of Defense information networks area of operation. Primarily we execute the command-and-control function for defensive cyberspace operations in support of the warfighter and our mission partners. More specifically, the DJOC Defensive Cyber Operations, or DCO Division empowers the cyberspace defense workforce to use DISA provided capabilities to maximum effect to simultaneously defend the DODIN area of operations, also known as DAO DISA and harmonize cybersecurity and the user experience.

As an enabler for warfighters and mission partners across the department, the DCO Division is highly focused on denying adversary access to DAO DISA by closing or mitigating vulnerabilities to DISA networks. Our actions often have effects well beyond DAO DISA in that our boundary section directs protections that benefit the entire Department of Defense.

With the knowledge that adversaries begin reconnaissance actions for vulnerabilities within 15 minutes of release, it is imperative for us to “know our terrain” and be able to scope vulnerabilities across DAO DISA within minutes and quickly put into place countermeasures or mitigations to deny access to our adversaries.

We are moving towards using data as a shared asset across both the network operations and DCO domains and using both commercial and government intelligence products to drive DCO actions and increase our velocity of action. We are also working closely with other operations centers across the agency to build a culture of trust and help eliminate institutional silliness.

As DISA migrates toward zero trust, the DCO team must be postured to operate and defend in a zero trust environment. We will also be prepared to take full advantage of transformative capabilities like artificial intelligence and machine learning as they become available in the DCO environment.

DAVID McCARTHY
Chief, Defensive Cyber Operations Division
DISA Joint Operations Center

DISA JOINT OPERATIONS CENTER

The DISA Joint Operations Center, or DJOC, is a key element in delivering shared transparency of understanding and driving actions across the globe by integrating across the agency's staff, field commands, field offices, service providers and mission partners within the current and future operations event horizons.

While the DJOC watch team and division cover the current operations events, the center's other divisions focus on future operations events on the horizon. Together, the team seeks to perfect operations by enabling and assuring the delivery, operation, defense and synchronization of capabilities and services that are available, reliable, and secure in support of the Department of Defense Information Network.

The DJOC manages the agency's operational battle rhythm, a deliberate recurring schedule of critical events at varying levels that are synchronized across internal and external stakeholders to regulate the flow of information. This capability is key in supporting the agencies and director's decision cycle in direct support to our mission partners. Our watch teams narrow the information gap and expand the visibility of the enterprise for our mission partners using command net, which is used to share operational data.

Additionally, the DJOC team works as the coordinating force for the agency, aligning DISA capabilities that enable combatant command mission essential functions through all phases of operations. In fact, our field and headquarters-based elements are vital to the assurance of global operational support to the warfighter. These "front-line" units provide vital information regarding operational impacts on service degradations and outages to inform the DISA enterprise situational awareness.

Looking ahead, we continue to identify opportunities to further leverage technology to more effectively collaborate and drive operational actions and activities across the agency. We are also looking forward to deploying automation for proactive sensing of our command-and-control environment to drive incident avoidance, rapid response and increased operational agility. DISA's Enterprise Integration and Innovation Center and Enterprise Engineering and Governance Directorate are driving the agency forward in this area and we look forward to continuing to work with them in this effort. These two efforts prioritize command and control and leveraging data as the center for gravity that will greatly increase our velocity of action and improve the services DISA provides to the warfighter..

U.S. NAVY CAPT. AARON LITTLEJOHN

Commander
DISA Joint Operations Center

DISA FIELD COMMANDS/FIELD OFFICES

DISA is a combat support agency that, as part of the U.S. Department of Defense, provides information technology (IT) and cyber solutions to America's Airmen, Guardians, Marines, Sailors and Soldiers. Thanks to the unique IT and cyber capabilities that DISA provides, the U.S. military can access and depend on secure, reliable and resilient communications infrastructure to conduct military operations across all domains – in the air, on land, at sea, in space and cyberspace. While the agency is headquartered at Ft. George G. Meade in Maryland, it maintains a global presence throughout Asia, Europe, the Middle East and North America.

Shown here are DISA's seven Network Operations Centers (gold) and 12 Field Offices (black) that combine to form DISA's Cyberspace Operations global footprint. Network Operations Centers, where the U.S. military's IT networks and computer systems are monitored and managed around the clock, serve as the first line of defense against disruptions and failures. Field Offices provide direct, embedded support to the 11 combatant commands, their subordinates and components, ensuring the seamless deployment of IT and cyber capabilities to the warfighter, anywhere in the world.

U.S. Air Force Col.

KELLY ROXBURGH-MARTINEZ

Commander

BEAU BUDER

Deputy Commander

The DISA NORTHCOM Field Office, which is collocated with the U.S. North American Aerospace Defense Command, or NORAD, and U.S. Northern Command at Peterson Space Force Base in Colorado, ensures that operational capabilities provided by DISA meet current needs and future needs of both organizations and serves as a knowledgeable advocate for the commands. In this vein we reach back to the agency headquarters at Fort Meade, Maryland, to resolve issues, submit requirements, broker solutions, and take actions that will optimize NORAD and USNORTHCOM's operational effectiveness.

Our collocation with NORAD and USNORTHCOM allows members of the DISA team to connect to and maintain day-to-day awareness of the commands' vision, priorities and technology roadmaps and provide proactive support as to new missions, including the U.S. Space Force and U.S. Space Command, which our field office has supported since its establishment in 2019.

Our support to NORAD is especially critical towards maintaining its bilateral warfighting posture with Canada. Through the five eyes, also known as FVEY, intelligence alliance, we ensure Canada's access to DISA services, in support of the multilateral treaty enabling sharing of signal intelligence between Australia, Canada, New Zealand, the United Kingdom and United States.

Looking ahead, DISA NORTHCOM will continue to facilitate sunsetting and transitioning new DISA capabilities year-after-year in support of NORAD and USNORTHCOM. This includes DISA's contribution to Joint All-Domain Command and Control, or JADC2, Project Thunderdome, Bring Your Own Authorized Device, DOD 365 on the Secret Internet Protocol Router Network to include FVEY authorized access, Joint Warfighter Cloud Capability, and soon Low Earth Orbit Satellite constellation gateways into the DISN.

NORTHCOM

U.S. Army Col.

DIANE E. KLEIN

Commander

DARREN FRIESZ

Deputy Commander

As the premier cyber and information technology forward presence and service provider for the Department of Defense in Europe, the DISA Europe Field Command operates, maintains and defends the globally interconnected DODIN that delivers digital information to warfighters on-demand; deploys enterprise solutions and capabilities, and executes unified command and control throughout the full spectrum of operations supporting U.S. European Command, U.S. Africa Command and other mission partners.

DISA Europe takes decisive action to deliver optimal support at speed. Recently, the field office was instrumental in saving 215 migrants at sea during the Afghanistan Non-Combatant Evacuation Operation, rescuing four high value assets during covert operations and proactively integrating into the USEUCOM Russia/Ukraine operational planning team in response to the Russian problem set. DISA Europe was also critical to the development of DISA's first force package to increase global command, control, communications, and computer, also known as C4, resiliency of the enterprise services and infrastructure utilized during any contingency operation and executed with the Ukraine crisis.

DISA Europe guided and assisted USEUCOM in the migration to DOD365-J email and voice tenants, enabling international calling capabilities into the Microsoft Teams meetings while seamlessly integrating a transition from the Army's email system to the DOD's.

Looking ahead, the future of DISA Europe is promising. We are committed to innovating, building partnerships and leading battle drills designed to prepare DISA for the possibility of conflict while enabling EUCOM to lead in all domains. DISA Europe will continue improving EUCOM's cyber protection by greatly increasing their defensive cyber defense, mitigating vulnerabilities and continuing to be their Cyber Security Service Provider of choice engaging mission partners,

HQ DISA and other stakeholders leading to a multitude of successful events and exercises while continuing to forge long lasting relationships.

EUROPE

JULIO FERRERIS
Acting Commander

To enable warfighting functions across U.S. Southern Command and its component commands and partner nations, the DISA South field office collaborates with domestic and international mission partners to plan, synchronize and direct DODIN operations and Defensive Cyberspace Operations-Internal Defense Measures. These efforts protect USSOUTHCOM's ability to utilize friendly cyberspace capabilities and protect their data, networks, net-centric capabilities, and mission-critical systems.

Our team at DISA South designs, engineers and oversees the installation of terrestrial fiber optic cables and satellite communication systems within the USSOUTHCOM headquarters and area of responsibility to increase the resiliency of command and control for humanitarian assistance and disaster recovery operations. During Haiti's earthquake in August 2021, we were responsible for the rapid procurement and installation of 10 gigabytes of circuit in support of the U.S. Agency for International Development's command and control efforts, turning contractual actions around in just 40 days instead of the standard 180 days.

Our DISA South team also leads the Combat Support Agency Review Team and J6 Command and Control Operational Summit conferences for DISA, ensuring that defensive cyberspace operations are synchronized with the user experience across all unified combatant commands and parent services.

Looking ahead, DISA South plans to increase staffing through surge packages that will provide additional defensive cyber operational support to US SOUTHCOM during contingencies and multilateral security cooperation exercises. We are also putting into operation the additional resiliency circuits designed by DISA South to enhance the command and control capabilities of USSOUTHCOM and its component commands through fiscal year 2025.

USSOUTHCOM

U.S. Navy Capt.
RALPH J. STEPHENS
Commander

JEAN A. ROBINSON
Deputy Commander

With a focus on delivering stellar customer service, the DISA Special Operations Command Field Office helps U.S. Special Operations Command and the 6th Air Refueling Wing successfully leverage DISA's enterprise solutions and capabilities to execute their garrison and deployed operations, maintain situational awareness of the DODIN, conduct integrated planning to assure enterprise solutions and capabilities in support of SOCOM and other mission partners.

Supporting USSOCOM's command and control requirements is a significant part of the field office's mission. DISA SOCOM provides 24/7 support for all the DISA services that USSOCOM uses and supports all of the command's transport and circuit requirements, assisting the circuit team with transition of more than 100 legacy time division multiplex circuits.

In support of USSOCOM, the field office also leans forward to promote DISA's emerging technologies. From their position of colocation with the command, the DISA team actively listens to USSOCOM's needs, proactively looks for opportunities where DISA solutions can meet USSOCOM requirements and presents information about available capabilities; often offering operationally effective solutions that USSOCOM can leverage instead of developing new ones.

Over the last year, the field office has strengthened their cybersecurity partnership with USSOCOM, adding a new cybersecurity position to their office in Fort Bragg, North Carolina. Looking ahead, the future for DISA SOCOM is bright and busy. DISA is increasingly integrated with the USSOCOM Airborne Intelligence, Surveillance and Reconnaissance team to ensure synchronization between organizations. One of teams' main priorities is to gain and maintain the trust and confidence of USSOCOM and where feasible, support them in their emerging technology initiatives, such a delivering cloud capability to the tactical edge.

USSOCOM

U.S. Air Force Col.

JASON MOBLEY

Commander

ANNETTE M. JORDAN, PH.D., CPWC

Deputy and Technical Director

The DISA Strategic Command Field Office operates an agile, high-caliber organization dedicated to ensuring that DISA's transport architecture is modernized and that national leader command capabilities support U.S. Strategic Command's mission.

We are vital to maximizing DISA's support to USSTRATCOM. In fact,our collocation with USSTRATCOM is the prime enabler to providing the command with rapid response, whether it's gathering operational requirements, supporting the delivery or implementation of new services, working technical problems, or providing 24/7 network operations support. We sit face-to-face with our USSTRATCOM mission partners, attend scheduled project, and staff meetings, and even synchronize efforts during informal hallway conversations.

The COVID-19 pandemic highlighted our value to USSTRATCOM as we worked side-by-side to enable technology for not only a mobile workforce, but a remote workforce that still needed some measure of access to classified systems to execute mission imperatives. we supported the command's implementation of Commercial Virtual Remote, the Microsoft Teams solution for unclassified collaboration put into place to support telework operations during the pandemic. As operations normalized, we pivoted and turned our focus to support USSTRATCOM's transition to DOD-365 Joint, working as a single project team to ensure that the command transitioned on-schedule.

In the future, we envision continued and growing support to our combatant command. In the coming year we expect to lead efforts towards transitioning to IL6 DOD 365, DOD's secure collaboration solution; support delivery of new national leader conferencing capability, continue to mature our 24/7 network operations support, assume responsibility for elements of USSTRATCOM's Cyber Security Service Provider program, increase use of DISA's NLCC TS/SCI system, and support implementation of Project Thunderdome.

USSTRATCOM

U.S. Air Force Col.

MICKEY R. EVANS

Commander

WILLIAM DEAGAN

Deputy Commander

We are at the tip of the spear for DISA serving as an enabler and advocate between our mission partners at U.S. Transportation Command and the larger DISA enterprise. In those roles, we work to maximize USTRANSCOM's success by leveraging DISA's services and capabilities.

We endeavor to ensure our mission partners are aware of DISA services that might satisfy their requirements and with a deep understanding of the mission partner's requirements, the team works vigorously to ensure issues are addressed before they escalate and when outages or issues do occur.

In September 2021, USTRANSCOM successfully executed the largest non-combatant evacuation operation in the command's history. Our office and the DISA enterprise enabled that success. Two of our team members were lauded by USTRANSCOM for the support they provided the command regarding Log4j mitigations.

If you were to ask anyone that has studied warfare to name two capabilities that are key to success on the battlefield, you would consistently hear logistics and communications. Positioned at the nexus of those two capabilities is the DISA TRANSCOM Field Office. What interests our mission partner, interests our field office; so, we are laser focused on identifying ways to provide agile and secure command and control, and modernize infrastructure and services. Right now, that means a transition to Enterprise Voice over Internet Protocol. In the future we expect this to include the transition to existing and emerging technologies such as DOD network, DOD365 on SIPR, IL6 cloud, expanded zero trust capability, better leveraging data and artificial intelligence for advanced decision making, as well other enterprise improvements and capabilities.

USTRANSCOM

CENTRAL

U.S. Army Col.
BRIAN KADET
Commander

The DISA Central Field Command is a microcosm of DISA, providing operational, engineering, human resources and planning support as it advocates DISA's services to our mission partners at U.S. Central Command. Our world-class, geographically dispersed workforce are empowered to innovate, recommend, and resolve technical and non-technical challenges at every level.

TANIA M. WILKES
Deputy Commander

Both the Tampa and Manama, Bahrain Network Operations Centers enable us to prioritize services with various customers located across Southwest Asia and USCENTCOM at MacDill Air Force Base in Tampa. Personnel at the DISA Central Bahrain Field Office, continue to stage and deploy field engineers to maintain forward equipment while upgrading legacy equipment to reduce vulnerabilities. This forward-deployed presence also supports a rapid response to outages to minimize downtime of services and quick reaction to possible threats on the network.

Our trusted relationship with the command allowed us to streamline reporting between USCENTCOM, U.S. Forces Afghanistan-Forward, the Army's Regional Cyber Command-Southwest Asia, and 82nd Airborne during the August 2021 retrograde and non-combatant evacuation operations evacuating more than 123,000 U.S. forces and civilians from Afghanistan. We also submitted more than one thousand Special Immigrant Visa requests through the Defense Security Cooperation Management Office-Afghanistan and the Department of State team supporting Afghan allies. DISA Central engaged in this heightened humanitarian effort while leading the USCENTCOM's adoption of DISA's Cloud-Based Internet Isolation service that secured USCENTCOM's critical web-based internet traffic.

In the future, the command will have ample opportunity to advocate and shape new requirements as the mission shifts within Southwest Asia and USCENTCOM. We believe a tighter, more blended work relationship with our mission partners will facilitate additional innovation and improved requirement forecasting.

PACIFIC

U.S. Marine Corps Col.
JARED VONEIDA
Commander

As the representative of DISA's equities across the world's largest geographic area of responsibility, the DISA Pacific regional field command directly supports U.S. Indo-Pacific Command and U.S. Forces Korea, operating a 24/7 DISA Network Operations Center in Hawaii and participating in the battle rhythm events held thrice weekly by the USINDOPACOM J6, the combatant command's senior military IT leader.

BRUCE A. MORGAN
Deputy Commander

DISA Pacific operates field offices forward deployed in Alaska, Guam, Hawaii, mainland Japan, Korea and Okinawa. Our agency ambassadors in each office act as DISA sensors – becoming the eyes, ears, hands, and feet in the region – and working side-by-side with our mission partners when necessary, we take direct action to provide onsite warfighter mission support in a timely and effective manner.

DISA Pacific connects over 265 DOD sites, supports 377,000 deployed forces, and operates across 16 time zones into the rest of the global DODIN. For the team at DISA Pacific, every calendar day begins in Guam and ends in Hawaii.

To ensure that USINDOPACOM maintains a high state of operational readiness, our DISA Pacific team resources and operates a leading quality assurance program. We execute an average of 55 performance evaluations a year – even extending our evaluation teams to visit key continental United States and Europe sites that connect back into our area of responsibility.

The future for DISA Pacific looks bright -- full of challenges and opportunities going forward. We see cloud as a warfighting enabler, allowing us to tie into global resources for assuring mission. Developing and deploying a "DISN Forward" capability, which will put together agnostic transport capabilities that allow warfighters to use any transport medium available, is another opportunity to capitalize on technology in assuring mission.

U.S. Army Col.

CHRISTOPHER MILLER

Commander

U.S. Air Force Senior Master Sgt.

MICHAEL MICHAUD

Senior Enlisted Leader

AFRICOM

The DISA Africa Command Field Office serves as the focal point for United States Africa Command, providing quality, timely information on cost-effective services to its components and other customers in the USAFRICOM area of responsibility. By serving as a liaison between USAFRICOM and other DISA elements, including the teams at DISA's headquarters in Fort Meade, Maryland, and DISA Global, the DISA AFRICOM Field Office can provide robust and timely support to the warfighter's mission.

DISA's support to the region includes enabling enhanced resiliency and survivability of the region's core infrastructure, providing cloud-based capabilities that are forward deployed, and making sure cybersecurity service provider services are expanded to include the multi-national networks shared with mission partners.

One of the most vital missions we support in this theater is Airborne Intelligence, Surveillance, and Reconnaissance connectivity, where older technologies are in the process of being phased out and replaced with a more resilient AISR-supporting infrastructure. One accomplishment we are most proud of was saving an American hostage rescue mission by ensuring AISR infrastructure was not inadvertently taken down by an untimely internal maintenance action.

Looking ahead, we believe that DISA AFRICOM's future is going to be as important as ever and maybe even more so. As Africa continues to be of strategic interest to our near peer adversaries, USAFRICOM will put more attention on countering those influences. With these adversaries' advanced cyberspace capabilities, we will need to stay one step ahead on ensuring DISA-provided infrastructure and services can meet that threat head on. We envision these to include, among others, enhanced resiliency and survivability of our core infrastructure, cloud-based capabilities that are forward deployed, and cybersecure service provider services expanded to include our multi-national networks we share with mission partners.

U.S. Army Col.

MIKE REEDER

Commander

DANA ROWE

Deputy Commander

GLOBAL

Headquartered at Scott Air Force Base, Illinois, DISA Global has been operating the Department of Defense's worldwide Internet Protocol infrastructure and services since its inception in 2003. The command is also continuing its ongoing work to accomplish full operational capability of its second global network operations center at Hill Air Force Base, Utah.

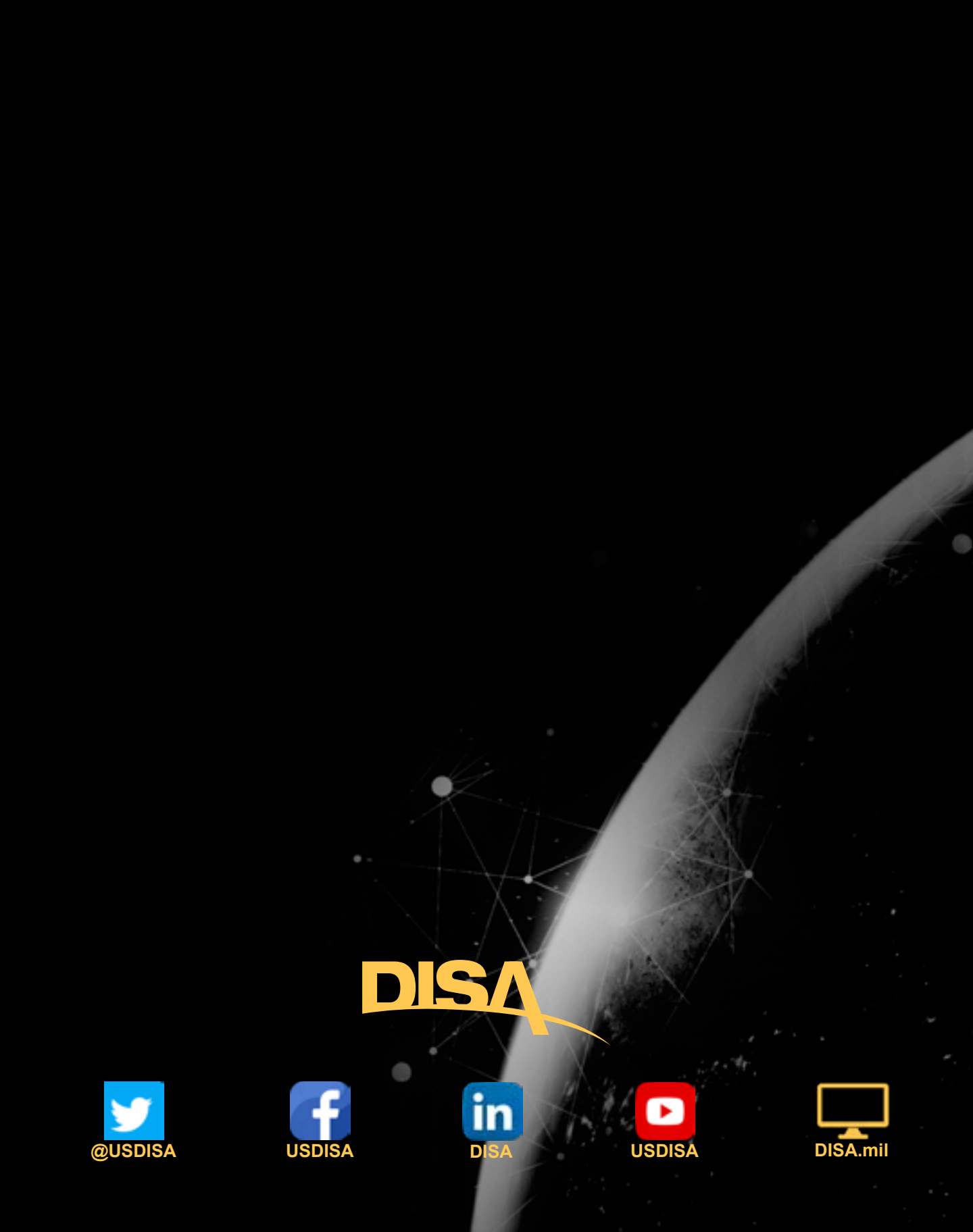
With a focus on global transport and boundary defense and a team of 1,300 federal civilian, military, and government contractor personnel, we provide critical and essential communication services to our national leadership and supported DOD organizations and monitor 40,000 miles of fiber-optic cables across the world.

In addition, DISA Global operates as one of the agency's largest operational service managers. This means that when the agency fields programs and technology, DISA Global is the operational service manager for those programs that fall within the transport or boundary defense. In 2021, we processed over 18,000 maintenance actions across the network and 60,000 customer incident tickets.

Alongside solving problems, we also conduct the defensive cyber operation monitoring of 10 internet access points, which handle more than 1,000 terabytes of data daily; ensuring that malicious actors aren't penetrating through the network.

Our collective goals are to provide timely, assured, and reliable capabilities to meet our national military objectives today and into the future.

DISA Global plays a key supporting role in DISA's shift toward its emerging zero trust network initiative, Project Thunderdome. This new security network design will move current network server-client security practices over and into one centered around the confidentiality, integrity, and audit-controlled availability of DOD data.


DISA
@USDISA
USDISA
DISA
USDISA
DISA.mil