Postured for Today's Competition & Ready for Tomorrow's Fight

Command Vision & Strategic Plan FY2022 -2024

Joint Force Headquarters Department of Defense
Information Network

About JFHQ-DODIN

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) drives unified actions to improve DODIN agility and resiliency to preserve mission assurance and bolster DoD's competitive advantage. As a component command of U.S. Cyber Command, JFHQ-DODIN's global command and control responsibility establishes a postured unified force approach to network operations, security and defense that enables active maneuver and rapid response across all DODIN areas of operations (DAOs). With each DAO commander and director responsible and accountable for their organization's DODIN terrain, JFHQ-DODIN integrates, synchronizes and directs priority actions to actively manage cyberspace risk to DoD core functions, missions and sectors.

Published October 2021

Commander’s Message

Joint Force Headquarters-Department of Defense Information Network’s top priority is the effective command and control of DODIN forces enabling mission assurance. This command vision provides our intent for the headquarters and mission area for the next three years.

Our fundamental critical success factors are agility, resiliency, velocity of action, boldness and accessibility to the DODIN. Our mission addresses complex issues 24 hours a day, 7 days a week and 365 days a year. The pace of operations does not afford the luxury of pausing as we explore solutions and implement change.

The great strategic power competition demands we remain postured for today’s competition while being ready for tomorrow’s fight. Consequently, we confidently move forward every day to continuously optimize the right mix of technology, talent, resources, policies, processes and partnerships.

I am excited about the future and JFHQ-DODIN’s ability to support DoD’s missions through a secure and defendable DODIN.

Respectfully,
Robert J. Skinner
Lieutenant General, USAF
Commander, JFHQ-DODIN

Executive Summary

JFHQ-DODIN enables commanders and directors to manage operational risk for mission assurance by understanding the readiness of the DODIN, threat conditions of the cyber environment and leveraging operational advantages as a unified force in cyberspace. The command integrates, synchronizes and directs the network operations, maintenance, security and defense of the DODIN. The urgency to work as a unified force is paramount because the DODIN underpins every DoD mission and is crucial to sectors' multi-domain operations.

Our work aligns with DoD's national defense strategy to optimize for long-term strategic competitive advantages. Our work supports the Secretary of Defense's three priorities—defend the nation, take care of our people and succeed through teamwork. Similarly, our work aligns with U.S. Cyber Command's 2021 Strategic Planning Guidance for operations and its vision for full-spectrum cyberspace operations through persistent engagement.

Srategic Focus Areas

This 2022-2024 JFHQ-DODIN Command Vision reflects the following vital points which are embedded in our four strategic focus areas:

- Streamline Command & Control
- Optimize Technology
- Harness the Power of Partnerships
- Cultivate Cultural Change & Talent Management

Underlying Vital Points

These strategic focus areas and the associated key activities reflect the following underlying vital points:

- Operating within the command-centric operational framework for cyber empowers and enables commanders and directors to decisively act as their cyberspace operations forces (COF) conduct network operations, security and defense of their DODIN areas of operation.
- Holistic continuous assessments of the DODIN terrain and force posture, reinforced through accountability, set the conditions for seamless simultaneous operations throughout DODIN's steady-state of continuous competition, and contingency and crisis situations.
- Increasing automation and leveraging technological capabilities, to the fullest extent possible, provides decision-makers with relevant operational data and threat-informed information to make timely operational and resource choices for mission assurance.
- Partnerships are powerful—period. The strategic environment requires relationships and cultural changes that acknowledge shared risks, express shared goals and seek shared solutions to stay ahead of adversaries.

Vision

Postured for today's competition and ready for tomorrow's fight.

Mission

JFHQ-DODIN effectively executes command and control by integrating, synchronizing and directing DODIN operations, security and defensive maneuvers to enable power projection and freedom of action across all warfighting domains.

Guiding Principles

Create Agility & Velocity

Operating as a unified force in steady-state competition against adversaries leads to economies of scale for cyberspace operations forces and enables them to thrive during times of uncertainty and crisis. This construct creates time and space for innovation to bolster decision-making with velocity, precision and inherent agility.

Prioritize Threats

Understanding adversaries' intent, capabilities and campaigns underpins the ability to prioritize resources and actions that protect critical DoD data, DODIN infrastructure and DODIN-enabled capabilities.

Secure & Advocate by Design

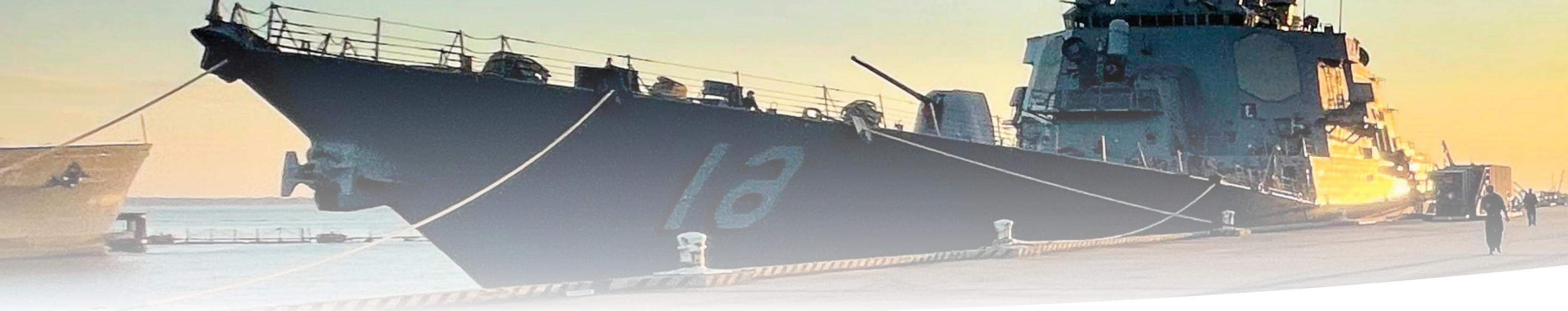
DoD cyberspace is best protected when all elements of the DODIN and the diverse DODIN-enabled capabilities are engineered and maintained for security throughout the design, development and operations lifecycle. Advocating for and supporting all DODIN areas of operation and sectors reinforces the importance of addressing priority needs as a unified force for developmental initiatives, policy, process changes and resources.

Embrace & Manage Risk

Real-time situational understanding of the cyber operational environment gives commanders and directors decision-quality information to make risk informed choices to continually improve their organization's posture.

Seamlessly Integrate

Integrating diversity of thought and experiences from the headquarters, components and mission partners enhances mission success.



The DODIN & Cyberspace Environment

Cyberspace is a precarious environment and the DODIN, DoD's cyber operational battlespace that underpins all DoD missions, is dynamic and ever-changing within the greater cyber landscape.

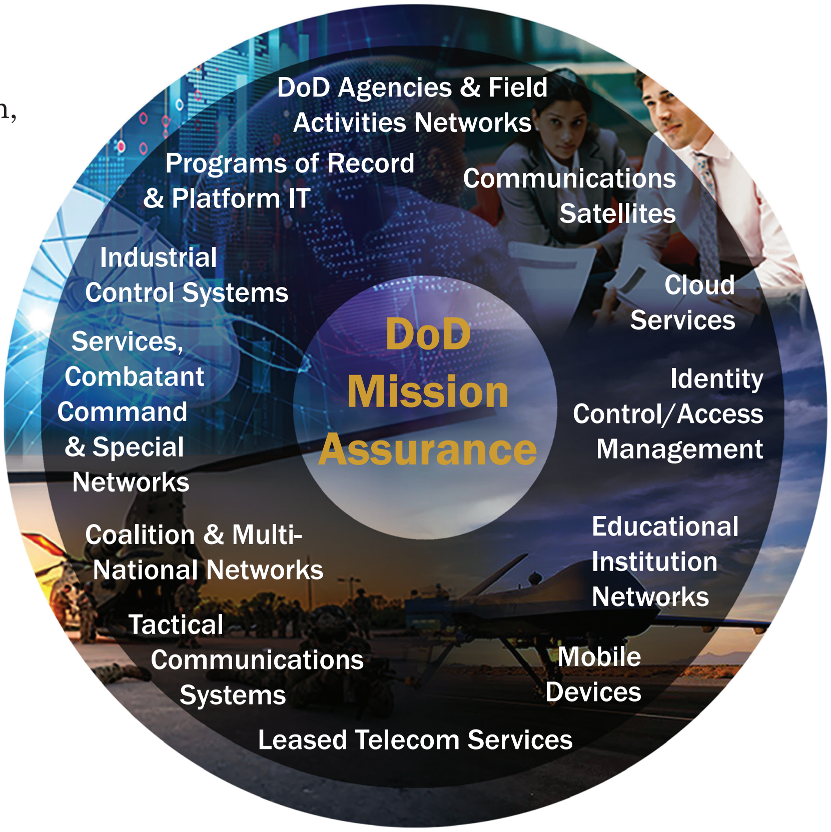
The DODIN is a continuously contested environment where adversaries operate at an advanced level in scope, scale and sophistication through both opportunistic and long-term malicious campaigns. They relentlessly aim to infiltrate the DODIN and supply chains to damage, disrupt, and manipulate information, missions, operations, weapons systems and partner relationships. As a result, the cyber environment is ubiquitously contested at all times, from the garrison to the combat zone.

To combat adversaries, JFHQ-DODIN leverages shared information while it directs, synchronizes and validates actions made by the DODIN areas of operations (DAOs) to reduce and harden the attack surfaces. Unity of action and coordination with partners are approaches intended to make attempting to attack the DODIN unattractive to adversaries because it increases their cost of resources and time; thus, outweighing the perceived benefits.

These efforts are integral to U.S. Cyber Command's persistent engagement approach with the concepts of anticipatory resilience, defend forward and contest actions.

The goal is to create a seamless transition between on-DODIN and off-DODIN activities.

Having a strong and secure infrastructure, coupled with diverse battle-ready protective measures, allows DoD to effectively deploy mission related maneuver efforts and cyberspace forces.


DoD Agencies & Field Activities Networks
Programs of Record & Platform IT
Communications Satellites
Industrial Control Systems
Cloud Services
Services, Combatant Command & Special Networks
DoD Mission Assurance
Identity Control/Access Management
Coalition & Multi-National Networks
Educational Institution Networks
Tactical Communications Systems
Mobile Devices
Leased Telecom Services

DODIN
Man-Made Global Federated Environment

45 areas of operation
15,000 networks
4 million computers*
3 million users*
300 terabytes of data daily across the DODIN*

****From Defense Information Systems Agency***

Where We Need To Be

The future DODIN architecture and operations must be based on a joint perspective for mission assurance supported by the integration of processes, technology development and employment, and human action in the operational environment. The purpose is to directly enable implementation and dynamic employment of a lethal joint force.

Enabling a Lethal Joint Force

Adaptable and defendable networks enable:

- Decisions that spark rapid response to cyber incidents
- Understanding of the dynamic cyber terrain and the interdependencies necessary in multi-domain operations
- Understanding adversary interests and targets
- Layered security and defense
- Aligning forces to essential missions with understanding of the relationship between readiness of the forces, cyber terrain and mission essential tasks

Necessary conditions include:

- A secure data-centric, zero-trust environment
- Common understanding of the operational risk—who is taking risk and who is responsible for the outcome
- Deconflicted statutes, policies and doctrine
- An operational mindset toward outcomes and capabilities oriented toward mission assurance, resourcing, operational decisions and priorities

Enabling Dynamic Force Employment

Threat and operationally informed decisions about network operations, security and defense of the DODIN enable:

- The capability to fully support the warfighter's transition to crisis contingency with near-peer competitors at little to no notice
- Integration with partner networks and capabilities, at notice to rapidly respond to missions where partner involvement is necessary
- The network architecture, DODIN-enabled capabilities and processes designed to rapidly support the movement of forces for priority operations

Necessary conditions include:

- Network operations, security and defensive priorities based on operational needs and requirements
- Common understanding of COF alignment, readiness and force posture
- Decisions about funding, resources, technology, policy and priority actions informed by threat conditions
- Integration of risk management and network operations, security and defensive actions enabling operational outcomes
- A combat development function for full-spectrum cyberspace operations
- Processes and tools for continuous assessment, tracking, reporting and aligning readiness of cyber terrain and assigned forces to operationally prioritized mission essential tasks across the four DoD core functions of warfighting, Services man/train/equip, DoD intelligence activities and business operations

Strategic Focus Areas

Streamline Command & Control

The command-centric operational framework for cyber is the linchpin that enables commanders and directors to achieve command and control over their DODIN terrain and cyberspace operational forces. It enables them to establish priorities for their mission area, and direct network operations, network security and network defense for their organization's mission assurance. JFHQ-DODIN will continually examine how we execute our supported role while fulfilling our supporting role for all sectors and DAOs. Additionally, JFHQ-DODIN's operational processes—including the cyber-risk assessment to mission methodology (C-RAMM) and the scope, assemble, score, relate-enforce (SASR-E) threat and vulnerability assessment methodology—must continue to evolve to optimize the command's supporting role to DODIN sectors.

Highlights of key activities:

- organizing the DODIN terrain, ensuring all terrain is assigned to the appropriate DoD component commander or director
- strengthening cyber intel and DODIN operations processes to enhance support to DODIN sectors and DAOs
- ensuring JFHQ-DODIN maneuver forces have the necessary capabilities to support DAO requirements
- enhancing and integrating training opportunities for COF to include cyberspace operations-integrated planning elements and DODIN maneuver forces

Optimize Technology

Sustainable network operations, security and defense hinges on refining processes, requirements and performance standards to meet operational needs. JFHQ-DODIN works across DoD to identify cyber requirements, optimize current capabilities to the fullest potential, and operationalize modernization efforts and new technology solutions. This involves seeing terrain, tools for automation, machine learning and artificial intelligence, and other DODIN-enabled capabilities across three horizons—existing, emerging and future. We will continue to advocate for components to identify and integrate enterprise level cyber capabilities designed to improve velocity of action, precision and agility.

Highlights of key activities:

- defining roles and standards associated with the DODIN operations, secure and defense of the DODIN mission area
- synchronizing zero trust principles in DODIN operations
- establishing a continuous and holistic assessment framework for DAOs that includes assessment of the DODIN terrain and force posture
- development of and leveraging a DoD-wide secure-operate-defend visualization capability that leads to situational understanding of the cyber environment including readiness of terrain and force posture, assessments, mission and terrain mapping, operational sensors, and threat informed priorities (e.g. Joint All-Domain Command and Control and Joint Cyber Warfighting Architecture)

Harness the Power of Partnerships

There is power in partnership. The strategic environment requires partnerships that acknowledge shared risks, express shared goals and seek shared solutions. We will prioritize partnership development to enhance collective defense, capacity and capability, and improve actions against adversaries. Critical elements of these partnerships involve the exchange of information about vulnerabilities, technical capabilities, processes and practices, and talent development. We will continue to build relationships, and identify and leverage partner authorities, responsibilities and capabilities to carry out our mission.

Highlights of key activities:

- driving revisions and establishing needed doctrine and policy to accurately reflect cyberspace operations and DODIN network, security and defense operations
- partnering with component commanders and directors, and other DoD entities, on processes that determine what is allowed to operate on the DODIN
- enhancing partnerships with the DoD components, CIO community, DoD intelligence community, National Security Agency Cyber Security Directorate and others on priority requirements for the mission area
- building and expanding relationships with external entities in academia, industry and commercial intelligence for expertise
- exploring information sharing opportunities and standards with international and coalition partnerships to strengthen operational dynamics and resiliency

Cultivate Cultural Change & Talent Management

Organizational culture and workforce competency significantly influence the effectiveness of mission assurance. They are essential factors that propel sustainable readiness. Our culture will be grounded with an operational perspective that allows us to most effectively execute our supported role while fulfilling our supporting role for all sectors and DAOs. We will operate with a culture of velocity, accountability, responsiveness and communication with components, partners and our workforce. We will look across the talent pool to ensure we have the right diversity of thought, education, subject matter expertise and competencies. Attracting and retaining high-end talent are important elements of our talent management approach that encompasses active duty, civilian, contract and reserve personnel.

Highlights of key activities:

- establishing qualification and performance standards leading to readiness of cyberspace operations forces bolstered by individual and collective training opportunities
- implementing a comprehensive human capital strategy
- instituting through DoD cyber academic programs a common understanding about DODIN operations, security and defense mission area concept of operations to promulgate common understanding of the command-centric operational framework for cyber
- pursuing collaborative training and education efforts with industry, academia, DoD organizations and other partners to generate a conveyor belt of talent trained and knowledgeable about the mission area; share expectations about workforce requirements

Way Ahead

This command vision outlines a bold strategic path to fulfilling our command and control mission as USCYBERCOM's operational arm protecting the DODIN. The efforts support the critical need for ongoing situational understanding of the cyberspace operating environment informing risk-to-mission decisions on a daily basis. We recognize the way ahead will continue to be dynamic and our four strategic focus areas are the broad guides that will keep us focused on the future.

The key activities listed are our priority targets for the next three years. Collectively they reflect critical themes for the headquarters and the mission area: promulgating and institutionalizing the command-centric operational framework across the cyberspace operational warfighting domain; establishing standards for forces and terrain, enhancing technology and automation, and leveraging continuous assessments and accountability that will shape cultural change across DoD. Progress toward the key activities will be measured by multiple factors and will drive our battle rhythm to enable timely adjustments.

JFHQ DODIN

Postured For Today's Competition. Ready For Tomorrow's Fight.