JFHQ-DODIN

Protecting DOD Networks for Mission Success

Strengthening Posture and Decreasing Risk

JFHQ-DODIN has a global command and control responsibility to establish a postured unified force approach for network operations, security activities, and defense across the Department of Defense Information network, commonly known as the DODIN, to improve network agility and resiliency to preserve mission assurance and bolster DoD's competitive advantage. Its mission covers a broad range of activities including proactive, threat-informed steps to reduce cyber risk across the DODIN, and leading DoD response to attacks against the DODIN to ensure DoD network operations remain agile and resilient.

JFHQ-DODIN Guiding Principles

Create Agility & Velocity

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

Understand Threat Environment

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

Secure & Advocate

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 DAOs 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 and threat environments gives commanders and directors decision-quality information to make risk-informed choices to improve their organization's posture.

Seamlessly Integrate

Critical thinking and integrating diversity of thought and experiences from the headquarters workforce, DODIN areas of operation and partners enhance mission success.

A Few Facts

- 15,000+ unclassified, classified, and special purpose networks and enclaves
- 230,000+ local defenders
- Dozens of internet access, strategic gateways and Cloud access points
- 38M incoming emails every day.
- 4M DOD computers
- 3.2M users
- 145K mobility devices

On Any Given Day . . .

- 798 million cybersecurity events
- 23.5 million marketing & phishing emails blocked
- 194 million malicious cyber attacks attempted

(Data from Defense Information Systems Agency)

JFHQ-DODIN is a Component-Command of U.S. Cyber Command

JFHQ DODIN

JFHQ-DODIN Lines of Effort

Our five lines of effort are critical aspects of full-spectrum cyberspace operations and include tasks for the headquarters and for the DODIN areas of operations and Sectors. They reinforce unity of command to compel action, enable accountability, optimize technology and shape cultural change across DoD.

BATTLESPACE COMMAND & CONTROL

The DODIN Areas of Operations are the centers of gravity for the secure, operate and defend the DODIN mission area. Their role is critical to managing cyber risk to DoD missions. The command-centric operational framework empowering and enabling commanders and directors to achieve unity of command and action to direct all DODIN cyberspace forces that conduct network operations, network security, and network defense for their area of responsibility. It enables DAO commanders and directors to support DODIN-wide requirements, Sector mission requirements and establish priorities for their own mission assurance.

ACTIVELY DEFEND

Actively defending the DODIN involves effectively and rapidly maneuvering forces and shaping or manipulating the terrain to obtain operational advantage. These actions are designed to impose cost to adversaries through a proactive unified force approach to on-DODIN operations. These activities are crucial to USCYBERCOM's full-spectrum cyberspace operations by creating a seamless transition between on-DODIN and off-DODIN activities. JFHQ-DODIN leverages unity of action across DAOs to direct daily operational activities and defensive actions to reduce and harden the attack surface, conduct countermeasures, mitigate vulnerabilities, remediate adversary attacks, manage a sensoring strategy, and leverage the cyber protection teams managed by various DoD organizations.

ENHANCING PARTNERSHIPS

The global strategic competition environment requires partnerships acknowledging shared risks, expressing shared goals and seeking shared solutions. Our internal-DoD partnerships center on developing common understanding to ensure technology and capability development, resource planning and support activities align with operational requirements. Our broad external reach focuses on strengthening relationships with U.S. federal agencies, allies, coalition, international partners, academia, Defense Industrial Base, and the commercial defense and technology sectors.

BUILD RESILIENCY

Resiliency refers to having strong networks and processes that can fully and quickly recover from an adversary's presence or attack. Speed of action is the driving force to ensure continuity of network, cyber security and defensive operations. JFHQ-DODIN proactively engages across DoD to identify cyber requirements for the mission area, optimize current capabilities and capacity to the fullest potential, and operationalize modernization efforts and new technology solutions and processes across three horizons—existing, emerging and future.

EMPOWER THE WORKFORCE

Workforce competency and organizational culture significantly influence DoD mission assurance. They are essential factors to ensuring the necessary operational perspective guides decision-making about emerging technologies and resources. We advocate for all decisions about the DODIN to be made with this operational perspective as the priority We seek the talent pool to ensure we have the right diversity of thought, education, subject matter expertise and competencies.