Department of War
Cyber Workforce Rotational Programs
Rotational Opportunity Details
2025-2026 Cohort

Rotation Opportunities Overview

The table below lists all the available rotation opportunities for the 2025-2025 cohort of the Cyber Workforce Rotational Programs. The hyperlinks embedded in the table will take you to the following areas:

- **Full Rotation Opportunity Details:** For more information, click the hyperlinked title of each opportunity to navigate to its full description within this document.
- **Application:** To apply to the opportunity, you can click the hyperlink embedded in the opportunity number to navigate to the application form.

Please be advised that for rotational assignments beyond a 50-mile commuting radius, your home organization will cover all approved Temporary Duty (TDY) expenses for the duration of the assignment.

Number	Host Organization	Division	Title	Location (s)
USMC-DoW-FRCWP-26-001	U.S Marine Corps (USMC) - Marine Corps Forces Cyberspace Command (MARFORCYBER)	G9, Development Operations Group	Cyberspace Capability Developer	Fort Meade, MD
DTIC-DoW-FRCWP-26-002	Defense Technical Information Center (DTIC)	N/A	Risk Management Framework (RMF) Control Assessor	Fort Belvoir, VA
DTIC-DoW-CITEP-26-003	Defense Technical Information Center (DTIC)	N/A	Cyber Auditor/Incident Response Analyst	Fort Belvoir, VA
DTIC-DoW-CITEP-26-004	Defense Technical Information Center (DTIC)	CIO	Risk Management Framework and FedRAMP Analyst	Fort Belvoir, VA
DTIC-DoW-CITEP-26-005	Defense Technical Information Center (DTIC)	CIO	Security Operations Center Analyst	Fort Belvoir, VA
DAF-DoW-CITEP-26-006	U.S Air Force - Headquarters Air Force A10	AF/A10XN - Strategic Deterrence and Nuclear Integration	Cybersecurity Specialist (Air Force A10XN Cyber Branch)	Pentagon (Arlington, Virginia)
CCMDS-DoW-FRCWP-26-007	U.S. European Command (USEUCOM)	ECJ68 - C4/Cyber Directorate	Mission Relevant Terrain in Cyber (MRT-C) Analyst	Stuttgart, Germany

DAF-DoW-FRCWP-26-008	Headquarters Space Force - Data, AI, and Software Directorate (SF/S6D)	Deputy Chief of Space Operations for Data and Cyber (SF/S6)	Artificial Intelligence Program Manager	Arlington, VA
CCMDS-DoW-FRCWP-26-009	U.S. Indo-Pacific Command (USINDOPACOM)	J6 - Command, Control, Communications and Cyber Directorate	INDOPACOM J6 - C4/Cyber mission enabler	CAMP H.M. Smith (Aeia, Hawaii)
DAF-DoW-CITEP-26-010	U.S Air Force - Air Force Operational Test & Evaluation Center (AFOTEC)	Communications & Information Directorate (A6)	IT Project Manager – Digital Transformation & Cybersecurity	Kirtland Air Force Base (Albuquerque, New Mexico)
DAF-DoW-CITEP-26-011	U.S Air Force - Air Force Operational Test & Evaluation Center (AFOTEC)	Directorate of Intelligence, Analyses, and Assessments (AFOTEC/A2/9)	AI Digital Transformation Specialist	Kirtland Air Force Base (Albuquerque, New Mexico)
DAF-DoW-CITEP-26-012	U.S Air Force - Air Force Operational Test & Evaluation Center (AFOTEC)	Air Force Operational Test and Evaluation Center Detachment 6	Data Subject Matter Expert	Nellis Air Force Base (Las Vegas, NV)
J1-DoW-FRCWP-26-013	Joint Chiefs of Staff - Directorate for Manpower and Personnel (J-1)	Personnel Readiness Division (PRD)	Personnel Accountability/Personnel Strength Reporting Data Analyst	Pentagon (Arlington, VA)
TRMC-DoW-FRCWP-26-014	Test Resource Management Center	National Cyber Range Complex	National Cyber Range Complex - Cyber Range Program Specialist	• Orlando, FL • Patuxent River, MD • Charleston, SC
DAF-DoW-CITEP-26-015	U.S Air Force - 333d Training Squadron	TRR – Curriculum development	Industry Cyber Training Specialist	Biloxi, MS
DCAA-DoW-FRCWP-26-016	Defense Contract Audit Agency (DCAA)	DCAA Office of Chief Information Officer	Information Systems Security Manager (CSSP)	• Irving, TX • Fort Belvoir, VA
DCAA-DoW-CITEP-26-017	Defense Contract Audit Agency (DCAA)	Office of Chief Information Officer (CIO)	Data Scientist	Fort Belvoir, VA
DCMA-DoW-FRCWP-26-018	Defense Contract Management Agency (DCMA)	Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)	Cybersecurity Specialist	Mobile work opportunity with up to 50% travel

DoN-DoW-FRCWP-26-019	U.S. Navy - Office of the Department of Navy Principal Cyber Advisor	Office of the Department of Navy Principal Cyber Advisor	Cyber Policy Analyst	Pentagon Building
DISA-DoW-FRCWP-26-021	Defense Information Systems Agency (DISA) - DISA Europe (No. 001)	Defensive Cyber Operations Branch	DISA Europe Fellowship	Patch Barracks, USAG Stuttgart, Germany
DISA-DoW-FRCWP-26-022	Defense Information Systems Agency (DISA) - DISA Europe (No. 002)	Defensive Cyber Operations Branch	DISA Europe Fellowship	Patch Barracks, USAG Stuttgart, Germany
DISA-DoW-FRCWP-26-023	Defense Information Systems Agency (DISA) - DISA Europe (No. 003)	Defensive Cyber Operations Branch	DISA Europe Fellowship	Patch Barracks, USAG Stuttgart, Germany
DISA-DoW-FRCWP-26-024	Defense Information Systems Agency (DISA) - DISA Europe (No. 004)	Future Operations	Change Management Coordinator	USAG Stuttgart, Germany
DISA-DoW-FRCWP-26-025	Defense Information Systems Agency - DISA Europe (No. 005)	Future Operations	Data Scientist or Data Analyst for DISA's first full-time Data Cell	USAG Stuttgart, Germany
DISA-DoW-FRCWP-26-026	Defense Information Systems Agency (DISA)	J5 Plans and Strategy/J53 Plans Integration	Data Analyst, a Data Operation Specialist, or a Strategic Planner/Coordinator	Fort Meade, Maryland
DISA-DoW-FRCWP-26-027	Defense Information Systems Agency (DISA)	J5 Plans and Strategy/J53 Plans Integration	Cyber Operations Planner	Fort Meade, Maryland
DAF-DoW-FRCWP-26-028	U.S. Air Force - 38th Cyberspace Operations Group	Engineering Squadron - Performance Monitoring - Data Analytics	Voice System Architect: US Installations in processing to fully VoIP/UC migration - 911 system	Tinker AFB, OK preferred (local site), but flexible to any location
DAF-DoW-FRCWP-26-029	U.S. Air Force - Space Systems Command	Systems Delta 85 - Global Mission Data Dominance	Data Operations Specialist	Peterson Space Force Base
DoWEA-DoW-CITEP-26-030	Department of War Education Activity (DoWEA)	IT Division	AI Solutions Architect	Alexandria, Va

DISA-DoW-FRCWP-26-031	Defense Information Systems Agency (DISA)	Europe Regional Field Command (EU4)	Knowledge Operations Manager	USAG Stuttgart-Patch Barracks, DE (No. 008)
DISA-DoW-FRCWP-26-032	Defense Information Systems Agency (DISA)	J7, Readiness Division	Cyber Exercise Planner	Fort George G. Meade, Maryland (No. 009)
DISA-DoW-FRCWP-26-033	Defense Information Systems Agency (DISA)	Cyber Security Service Provider	Mission Partner Liaison	Chambersburg, Pennsylvania (Letterkenny Army Depot)
DISA-DoW-FRCWP-26-034	Defense Information Systems Agency (DISA)	DISA Global Field Command, Operations Division	AI Machine Learning	Scott AFB, Illinois 62225 and/or Defense Supply Center Columbus, Ohio 43213 (No. 11)
DA-DoW-FRCWP-26-035	U.S. Army - Department of the Army (DA)	Network Command (NETCOM)	Analyst	• Fort Huachuca, AZ • Schofield Barracks, HI • Cam Humphreys, ROK • Wiesbaden, Germany
DISA-DoW-FRCWP-26-036	Defense Information Systems Agency (DISA)	DISA Global Field Command, Operations Division	Cybersecurity Watch Officer	Scott AFB, Illinois 62225, and/or Defense Supply Center Columbus, Ohio 43213 (No. 12)
DA-DoW-FRCWP-26-037	U.S. Army - Department of the Army (DA)	Army Cyber Command Headquarters	ArCTIC – Research and Innovation Program Manager	Augusta, GA
DISA-DoW-FRCWP-26-038	Defense Information Systems Agency (DISA)	Europe Field Command, EU33 Current Operations	DISN Netops Center Battle Captain	Patch Barracks, USAG Stuttgart, Germany (No. 13)
DA-DoW-FRCWP-26-039	U.S. Army - Department of the Army (DA)	Army Cyber Headquarters	Data Warfare Division – Data Engineering	Augusta, GA
DA-DoW-FRCWP-26-040	U.S. Army - Department of the Army (DA)	Army Cyber Command (ARCYBER)	Data Warfare Division – Integration and Development of AI Enabled Applications	Augusta, GA
DA-DoW-FRCWP-26-041	U.S. Army - Department of the Army (DA)	Army Cyber Command (ARCYBER)	Cyber Protection Brigade - Cyber Defense Analytics and Hunt	Augusta, GA

USMC-DoW-FRCWP-26-042	U.S. Marine Corps - Deputy Commandant for Information (DC I)	Information Command, Control, Communications, and Computers (IC4)	Information Technology Specialist (Policy and Plans)	HQMC, Pentagon, DC
USMC-DoW-FRCWP-26-043	U.S. Marine Corps - Deputy Commandant for Information (DC I)	Information Command, Control, Communications, and Computers (IC4)	Enterprise Strategy Manager	HQMC, Pentagon, DC
USMC-DoW-FRCWP-26-044	U.S. Marine Corps - Deputy Commandant for Information (DC I)	Information Workforce Division (IWD)	Marine Corps Cyberspace Workforce Talent Management	HQMC, Pentagon, DC
J6-DoW-FRCWP-26-045	Joint Staff J-6	J6 - Command, Control, Communications & Computers (C4) / Cyber, Cyber & Information Systems Division (CISD)	Joint Staff J6 Cyber Rotational Position	Pentagon
USMC-DoW-FRCWP-26-046	U.S. Marine Corps - Deputy Commandant for Information (DC I)	Information Workforce Division (IWD)	Tactical Cyber Integration	• Camp Pendleton, CA • Camp Lejeune, NC • Pentagon, DC
CAN-IN-CITEP-26-047	Canfield Consulting Group, LLC d/b/a Canfield CyberDefense Group (CCG)	Division of Information Security Technology (DIT)	Canfield Cyber Defense Group (CCG)	Rockville, MD
USN-DoW-FRCWP-26-048	U.S. Navy	PEO Digital	Multiple (Solution Train Management/Agile Release Trains; NEN Directorate; Enterprise IT Contracting aaS)	WNY Bldg 196, Floor 3, Suite 301

Rotation Opportunity Descriptions

Opportunity Number: USMC-DoW-FRCWP-26-001

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – USMC-DoW-FRCWP-26-001

Host Organization

Name: United States Marine Corps (USMC) - Marine Corps Forces Cyberspace Command (MARFORCYBER)

Division: G9, Development Operations Group

Mission: MARFORCYBER enables full spectrum cyberspace operations, to include the planning and direction of Marine Corps Enterprise Network Operations (MCEN Ops) and defensive cyberspace operations (DCO) in support of Marine Corps, Joint and Coalition Forces, and the planning and, when authorized, direction of offensive cyberspace operations (OCO) in support of Joint and Coalition Forces, in order to enable freedom of action across all warfighting domains and deny the same to adversarial forces.

Vision: The MARFORCYBER G9 Development Operations Group provides software and hardware capabilities that produce cyberspace effects in and throughout cyberspace operations through vulnerability analysis, and software research and development.

Rotation Opportunity

Title: Cyberspace Capability Developer

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyberspace Capability Developer (341)
- Software Engineering - DevSecOps Specialist (627)
- Software Engineering - Software Test & Evaluation Specialist (673)

Location: Fort Meade, Maryland

Work Schedule: Candidates will be able to use a MaxiFlex work schedule with core hours dictated by project assignment. Core hours are typically 10AM-2PM to account for sprints, meetings, and collaboration.

Travel Requirements: Not Required

Duration: 12 Months

Description: Candidates will be a part of the G9 Development Operations Group and will help provide software and hardware capabilities that produce cyberspace effects to the Cyberspace Operators of MARFORCYBER and USCYBERCOM.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: The KSAs and Expertise desired can be best articulated via the respective DCWF Work Roles - 341 "Cyberspace Capability Developer" , 627 DevSecOps Specialist, or 673 "Software Test and Evaluation Specialist". These can be found here:

https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework/dcwf

Generally speaking, we are looking for candidates experienced with formal capability development practices, enabling software development (CI/CD, etc), or testing developed software to ensure rigorous adherence to USCYBERCOM standards.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: SCI / CI Poly will be required for use of systems and facility access.

Back to Top

Opportunity Number: DTIC-DoW-FRCWP-26-002

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DTIC-DoW-FRCWP-26-002

Host Organization

Name: Defense Technical Information Center (DTIC)

Division: N/A

Mission: The DTIC is the central repository for Research and Engineering (R&E) information for the Department of War (DoW). Its mission is to preserve, curate, and share knowledge from DoW's $20B/year investment in S&T, multiplying the value and accelerating capability to the warfighter. As a DoW field activity reporting to the Under Secretary of Defense for Research and Engineering (USD(R&E)), DTIC supports the USD(R&E)'s efforts to mitigate new and emerging threat capabilities, enable affordable or extended capabilities in existing military systems, and develop technology surprise through engineering by preserving and disseminating the research that led to the technologies warfighters use today; delivering the tools and collections that empower the R&E enterprise to accelerate the development of technologies that will help maintain the nation's technical superiority; stimulating innovation by providing access to DoW-funded research and digital data to the public and industry; and maximizing the value of each dollar the DoW spends through the analysis of funding, work-in-progress, and Independent Research and Development (IR&D) data to identify gaps, challenges, and way forward.

Vision: The defense research and development (R&D) recognizes DTIC as the provider of choice for defense research information, knowledge sharing, and advanced analysis.

Rotation Opportunity

Title: Risk Management Framework (RMF) Control Assessor

DoW Cyber Workforce Framework (DCWF) Work Role Code(s): Cybersecurity - Security Control Assessor (612)

Location: Ft. Belvoir, VA

Work Schedule: 100% onsite

Travel Requirements: Not Required

Duration: 12 months

Description: As an RMF Control Assessor, you will bring your skills and training to bear to ensure the confidentiality, integrity, availability and non-repudiation of DTIC's mission applications in the cloud. You will work side-by-side with the Center's professional cyber staff, application developers and testers, and DevSecOps engineers implement continuous authority to operate (cATO) dashboards and automation. You will apply programming standards and conventions, while identifying violations limiting or preventing code efficacy. You will mature your understanding of computers and computer science topics such as networking, database security, computer forensics, and cryptography as you develop and present risk recommendations to Information Systems Security Manager and Chief Information Officer.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Expertise in eMASS tool and APIs
- Build monitoring dashboards problems within code unrelated to security
- Script search for problems within code that expose private information or allow unauthorized access
- May perform penetration tests, review authorization protocols, and assess authentication mechanisms.
- Prepare oral and written reports on their findings
- Relay information to technical and non-technical colleagues

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: DTIC is a technology organization, focused on accelerating the flow of information within the DoW and with partners in industry and academia. DTIC is the Google/Wikipedia for the Department of Defense, providing actionable S&T information to support and spur research innovation, and allow the research and engineering community to build on the DoW's multi-billion-dollar annual investment in science and technology. DTIC collects, disseminates, and analyzes scientific and technical (S&T) information to rapidly and reliably delivers knowledge that propels development of the next generation of Warfighter technologies. With over four million records in its collection, DTIC is the largest central resource for defense and government-funded scientific, technical, engineering, and business-related information.

DTIC is also among the smallest of the DoW agencies which gives us the flexibility to work very informally across all levels of the agency. We have senior leaders and staff at all levels ready to support the Fellows. We appreciate what a precious resource the Fellows are, and we are committed to them having positive experiences with successful outcomes, for them and us.

Rotational programs such as FRCWP bolster our ability to quickly deploy those resources against time-sensitive problem sets – the novel skills possessed by junior professionals are often at the cutting-edge of technology and can drive innovation and technological change within organizations who may be unaware of such advances.

We have sponsored, and plan to continue sponsoring, US Digital Corps, Cyber Talent and AI Initiative, National Security Innovation Network (NSIN) X-Force Fellows, Presidential Management Fellows, American Association for the Advancement of Science (AAAS) Science

& Technology Policy Fellows, and Wounded Warriors who continually impress us with their professionalism, creativity and enthusiasm to tackle hard problems.

Back to Top

Opportunity Number: DTIC-DoW-CITEP-26-003

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DTIC-DoW-CITEP-26-003

Host Organization

Name: Defense Technical Information Center (DTIC)

Division: N/A

Mission: The Department of War (DoW) mission is to provide the military forces needed to deter war and ensure our nation's security. The Under Secretary of Defense Research and Engineering's Defense Technical Information Center (DTIC) is the central repository for Research and Engineering (R&E) information for the DoW. Its mission is to preserve, curate, and share knowledge from DoW's $20B/year investment in Science and Technology, multiplying the value and accelerating capability to the warfighter. As a DoW field activity reporting to the Under Secretary of Defense for Research and Engineering (USD(R&E)), DTIC supports USD(R&E)'s efforts to identify new and emerging capabilities, enable improved capabilities in existing military systems, and leverage DoW research products to develop new technologies for our warfighters. DTIC delivers knowledge discovery tools that exploit R&E collections to accelerate technology development and maintain our nation's technical superiority. DTIC solutions stimulate innovation through access to DoW-funded research and digital data sets to government, industry, and public partners. DTIC maximizes the value of each dollar spent by DoW through careful linking and analysis of funding data, program and project data, and Independent Research and Development (IR&D) data to identify gaps and make data-informed decisions on the way forward.

Vision: The Defense research and development (R&D) community recognizes DTIC as the provider of choice for defense research information, knowledge sharing, and advanced analysis.

Rotation Opportunity

Title: Cyber Auditor/Incident Response Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Cyber Defense Analyst (511)
- Cybersecurity - Cyber Defense Incident Responder (531)

Location: Ft. Belvoir, VA

Work Schedule: 100% onsite work

Travel Requirements: Not required

Duration: 12 months

Description: As a Cyber Auditor/Incident Response Analyst, you will bring your skills to bear ensuring DTIC's data assets are protected from unauthorized access, audit cloud infrastructure configurations, perform analysis against metrics and data, and finding and mitigating risks. You will mature your understanding of computers and computer science topics such as networking, database security, computer forensics, and cryptography as you develop and present risk recommendations to Information Systems Security Manager and Chief Information Officer.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Monitor security access
- Conduct security assessments through vulnerability testing and risk analysis
- Perform internal and external security audits
- Analyze security incidents
- Verify the security of commercial products and cloud solutions
- Recommend security architecture enhancements

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: DTIC is a technology organization, focused on accelerating the flow of information within the DoW and with partners in industry and academia. DTIC is the Google/Wikipedia for the Department of Defense, providing actionable S&T information to support and spur research innovation, and allow the research and engineering community to build on the DoW's multi-billion-dollar annual investment in science and technology. DTIC collects, disseminates, and analyzes scientific and technical (S&T) information to rapidly and reliably delivers knowledge that propels development of the next generation of Warfighter technologies. With over four million records in its collection, DTIC is the largest central resource

for defense and government-funded scientific, technical, engineering, and business-related information.

DTIC is also among the smallest of the DoW agencies which gives us the flexibility to work very informally across all levels of the agency. We have senior leaders and staff at all levels ready to support the Fellows. We appreciate what a precious resource the Fellows are, and we are committed to them having positive experiences with successful outcomes, for them and us.

Rotational programs such as FRCWP bolster our ability to quickly deploy those resources against time-sensitive problem sets – the novel skills possessed by junior professionals are often at the cutting-edge of technology and can drive innovation and technological change within organizations who may be unaware of such advances.

We have sponsored, and plan to continue sponsoring, US Digital Corps, Cyber Talent and AI Initiative, National Security Innovation Network (NSIN) X-Force Fellows, Presidential Management Fellows, American Association for the Advancement of Science (AAAS) Science & Technology Policy Fellows, and Wounded Warriors who continually impress us with their professionalism, creativity and enthusiasm to tackle hard problems.

Back to Top

Opportunity Number: DTIC-DoW-CITEP-26-004

Anticipated Start Date: July 27, 2026

Apply Here: **Cyber Rotation Programs Application – DTIC-DoW-CITEP-26-004**

Host Organization

Name: Defense Technical Information Center (DTIC)

Division: CIO

Mission: The DTIC is the central repository for Research and Engineering (R&E) information for the Department of War (DoW). Its mission is to preserve, curate, and share knowledge from DoW's $19B/year investment in S&T, multiplying the value and accelerating capability to the warfighter. As a DoW field activity reporting to the Under Secretary of Defense for Research and Engineering (USD(R&E)), DTIC supports the USD(R&E)'s efforts to mitigate new and emerging threat capabilities, enable affordable or extended capabilities in existing military

systems, and develop technology surprise through engineering by preserving and disseminating the research that led to the technologies warfighters use today; delivering the tools and collections that empower the R&E enterprise to accelerate the development of technologies that will help maintain the nation's technical superiority; stimulating innovation by providing access to DoW-funded research and digital data to the public and industry; and maximizing the value of each dollar the DoW spends through the analysis of funding, work-in-progress, and Independent Research and Development (IR&D) data to identify gaps, challenges, and way forward.

Vision: We seek candidates with a passion for leveraging technology to work alongside our team of library science, scientific, and technical professional to leverage software in support of the DoW S&T community which strives to convert research and engineering into capabilities that provide America's Warfighters with the competitive advantage needed to win on distant battlefields.

Rotation Opportunity

Title: Risk Management Framework and FedRAMP Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Security Control Assessor (612)
- Cybersecurity - Secure Software Assessor (622)
- Software Engineering - DevSecOps Specialist (627)

Location: Fort Belvoir, VA

Work Schedule: Onsite, flexible work schedules available

Travel Requirements: Not required

Duration: 6-12 months

Description: Join a comprehensive RMF program that aligns with the organization's risk tolerance and business objectives. Work shoulder to shoulder with a cadre of DoW cyber professionals at the forefront of assessing and authorizing cloud and software-as-a-service offerings. In this capacity you will engage directly with cloud service providers and increase the availability and diversity of advanced commercial capabilities to support DoW missions.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Learn the various pathways CSPs may pursue to obtain FedRAMP authorization, working with 3PAOs, the in's and out's of the DoW SaaS

authorization process, how to assess cloud applications and environments for use with sensitive and classified data, and more!

Desired Number of Participants: 3

Security Clearance Requirement: Secret

Special Requirements/Other: Bring your skill in analyzing problems and developing innovative and effective solutions (application of new program methods, approaches, and "state of the industry" cyber practices of information and educational technology) to improve efficiency, effectiveness, and policies and operations at DTIC!

Back to Top

Opportunity Number: DTIC-DoW-CITEP-26-005

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DTIC-DoW-CITEP-26-005

Host Organization

Name: Defense Technical Information Center (DTIC)

Division: CIO

Mission: The DTIC is the central repository for Research and Engineering (R&E) information for the Department of War (DoW). Its mission is to preserve, curate, and share knowledge from DoW's $19B/year investment in S&T, multiplying the value and accelerating capability to the warfighter. As a DoW field activity reporting to the Under Secretary of Defense for Research and Engineering (USD(R&E)), DTIC supports the USD(R&E)’s efforts to mitigate new and emerging threat capabilities, enable affordable or extended capabilities in existing military systems, and develop technology surprise through engineering by preserving and disseminating the research that led to the technologies warfighters use today; delivering the tools and collections that empower the R&E enterprise to accelerate the development of technologies that will help maintain the nation's technical superiority; stimulating innovation by providing access to DoW-funded research and digital data to the public and industry; and maximizing the value of each dollar the DoW spends through the analysis of funding, work-in-progress, and Independent Research and Development (IR&D) data to identify gaps, challenges, and way forward.

Vision: We seek candidates with a passion for leveraging technology to work alongside our team of library science, scientific, and technical professional to leverage software in support of the DoW S&T community which strives to convert research and engineering into capabilities that provide America's Warfighters with the competitive advantage needed to win on distant battlefields.

Rotation Opportunity

Title: Security Operations Center Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Exploitation Analyst (121)
- Cybersecurity - Cyber Defense Analyst (511)
- Cybersecurity - Vulnerability Assessment Analyst (541)

Location: Fort Belvoir, VA

Work Schedule: Onsite, flexible work schedules available

Travel Requirements: Not required

Duration: 6-12 months

Description: Conduct systems security evaluations, audits, and reviews to assess security events, determine impact, and implement corrective actions. Work shoulder to shoulder with a cadre of DoW cyber professionals charges with software factory security oversight and securing and defending cloud and software-as-a-service offerings. In this capacity you will engage directly with cloud service providers as you work to improve the cyber posture of gov clouds and developed code/applications to support DoW missions.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Learn to protect information systems and assets by leveraging vulnerability scanning tools, macro and micro risk assessment to understand risk in the broader operation context, identify and design vulnerability mitigations, stay up to date on the latest vulnerabilities, techniques for discovering new vulnerabilities, and more!

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: Bring your skill in analyzing problems and developing innovative and effective solutions (application of new program methods, approaches, and "state

of the industry" cyber practices of information and educational technology) to improve efficiency, effectiveness, and policies and operations at DTIC!

Back to Top

Opportunity Number: DAF-DoW-CITEP-26-006

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-CITEP-26-006

Host Organization

Name: Headquarters U.S Air Force A10

Division: AF/A10XN (Strategic Deterrence and Nuclear Integration)

Mission: AF/A10 conducts indefinite guidance, oversight, and advocacy of the Air Force strategic deterrence mission, in order to ensure Airmen have the necessary capabilities to protect the United States.

A10XN Mission: Lead Air Force advocacy and coordination to deliver credible information to Senior Leaders to define and defend NC3 sustainment, modernization, and integration with future operating concepts

Vision:

AF/A10 Vision: An Agile, back-to-basics directorate, ensuring safe, secure, and reliable deterrence both today and into the future.

A10XN Vision: Accurate data influencing the fielding of NC3 Weapon Systems to remain ahead of emerging threats and address end-of-life challenges

Rotation Opportunity

Title: Cybersecurity Specialist (Air Force A10XN Cyber Branch)

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyber Operations Planner (332)

- Cybersecurity - Cyber Defense Incident Responder (531)
- Cybersecurity - Vulnerability Assessment Analyst (541)
- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)

Location: Pentagon (Arlington, Virginia)

Work Schedule: 5-days on-site, with situational telework possible

Travel Requirements: Up to 50% depending on office needs

Duration: 9-12 months

Description:

- Collaborate with top-tier cybersecurity experts in the Department of War (DoW).
- Contribute to the security and modernization of critical NC3 systems that support national defense.
- Gain unique insights into government cybersecurity operations and challenges.
- Share innovative ideas and solutions to enhance the cybersecurity posture of NC3 systems.
- Collaborate with stakeholders across the Air Force and DoW to align cybersecurity efforts with NC3 objectives.
- Shape and advocate for policies that address cybersecurity challenges in NC3 systems, including Zero Trust paradigms and cyber hygiene.
- Conduct vulnerability assessments and provide actionable recommendations to enhance system security.
- Support real-time threat monitoring and advocate for advanced cybersecurity methods and funding.
- Educate internal and external stakeholders on NC3 cybersecurity systems, efforts, and challenges.
- Perform as a staff officer, preparing read ahead material and briefing material for Senior Leaders on a weekly basis.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Technical Expertise: Proficiency in cybersecurity principles, tools, and technologies.
- Policy Development: Experience in shaping and implementing cybersecurity policies and strategies at any level of implementation.
- Collaboration: Ability to work across diverse teams and organizations, including government and private sector partners.
- Communication: Strong written and verbal communication skills to advocate for cybersecurity initiatives and educate stakeholders.

- Problem-Solving: Analytical skills to address complex cybersecurity challenges and develop innovative solutions.
- Leadership: Demonstrated ability to lead teams and coordinate efforts across multiple organizations.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: This is more than just a rotation opportunity—it's a chance to make a meaningful impact on national security while gaining unparalleled experience in government cybersecurity operations. By joining the A10XN Cyber Branch, you'll be at the forefront of efforts to secure and modernize critical systems that support the nation's defense.

This version emphasizes collaboration, innovation, and the unique benefits of working with the Air Force and DoW, making it more appealing to private sector professionals. Let me know if further refinements are needed!

Back to Top

Opportunity Number: CCMDS-DoW-FRCWP-26-007

Anticipated Start Date: July 27, 2026

Apply Here: **Cyber Rotation Programs Application – CCMDS-DoW-FRCWP-26-007**

Host Organization

Name: U.S. European Command (USEUCOM)

Division: ECJ68 - C4/Cyber Directorate - Projects, Engineering, and Enterprise Architecture

Mission: USEUCOM executes a full range of multi-domain operations in coordination with Allies and partners to support NATO, deter Russia, assist in the defense of Israel, enable global operations, and counter trans-national threats in order to defend the Homeland forward and fortify Euro-Atlantic security. Should deterrence fail, USEUCOM is prepared to fight alongside Allies and partners to prevail in any conflict.

Vision: USEUCOM is a combat-ready, warfighting theater that is postured, relevant, and ready. We are united with our Allies and partners, prepared to execute the full range of combined and

Joint military operations, and capable of delivering decisive battlespace effects, at speed, and in all domains.

Rotation Opportunity

Title: Mission Relevant Terrain in Cyber (MRT-C) Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyber Operations Planner (332)
- Cyberspace Effects - Network Analyst (443)
- Cybersecurity - Cyber Defense Analyst (511)
- Cybersecurity - Cyber Defense Infrastructure Support Specialist (521)
- IT (Cyberspace) - Enterprise Architect (651)

Location: Stuttgart, Germany

Work Schedule: On-site 5 days a week

Travel Requirements: Not required

Duration: 6 months

Description: The MRT-C Analyst will be responsible for identifying, analyzing, and prioritizing mission-relevant cyber terrain within USEUCOM's operational environment. This individual will play a critical role in ensuring the cybersecurity posture of USEUCOM by mapping cyber dependencies, assessing risks, and recommending mitigation strategies to protect mission-critical systems and networks. The analyst will collaborate with cross-functional teams, including cybersecurity, intelligence, and operations personnel, to ensure mission assurance and operational resilience.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: The MRT-C Analyst for USEUCOM is expected to possess deep knowledge of cybersecurity principles, mission assurance, network architecture, and military operations, with experience in identifying and mapping mission-relevant cyber terrain. They should have strong analytical, technical, and communication skills to conduct risk assessments, prioritize vulnerabilities, and provide actionable recommendations to leadership. Collaboration and teamwork are essential, as the analyst will work with cross-functional teams and allied forces to ensure mission-critical systems are protected. The role requires adaptability, attention to detail, and strategic thinking to align cybersecurity efforts with operational priorities. Experience with Model-Based Systems Engineering (MBSE) and the Unified Architecture Framework (UAF) is critical for developing structured models and frameworks to analyze

mission dependencies and cyber terrain effectively. Certifications such as CISSP, CEH, or CompTIA Security+ are highly desirable, along with experience in military cyber operations and operational resilience.

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DAF-DoW-FRCWP-26-008

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-FRCWP-26-008

Host Organization

Name: Headquarters Space Force - Data, AI, and Software Directorate (SF/S6D)

Division: Deputy Chief of Space Operations for Data and Cyber (SF/S6)

Mission: Serves as the USSF Enterprise lead making data visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS), and serves as USSF focal point for Artificial Intelligence and Machine Learning activities supporting all USSF requirements.

Vision: To become a more data-driven, AI-enabled force able to conduct operations in contested and congested environments.

Rotation Opportunity

Title: Artificial Intelligence Program Manager

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623)
- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)
- Data/AI - AI Adoption Specialist (753)
- Cyberspace Enablers - Program Manager (801)

- Data/AI - AI Innovation Leader (902)

Location: Arlington, VA

Work Schedule: 5 days on-site, situational telework will be approved on a case-by-case basis.

Travel Requirements: Yes, but limited (approx. 10%)

Duration: 6-12 months

Description: This position is responsible for developing, implementing, and overseeing policies and governance frameworks for the effective management and use of Artificial Intelligence (AI) within the Space Domain. Supports the integration of AI-dependent solutions into Space Force operations, ensuring data architectures enable advanced analytics and decision-making capabilities.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge: Understanding of AI technologies, including machine learning (ML), natural language processing (NLP), computer vision, and predictive analytics. Ability to serve as a subject matter expert on AI technologies, data management, and digital transformation. Familiarity with AI development lifecycles, algorithms, and frameworks. Knowledge of ethical AI principles, responsible AI frameworks, and governance policies. Awareness of applicable policies, directives, and governance structures related to AI and emerging technologies.
  Skills: Skilled in aligning AI initiatives with organizational goals and mission priorities. Proficiency in managing large-scale AI programs, including planning, execution, and evaluation. Comfortable engaging with senior leaders, mission partners, and external stakeholders to promote AI adoption and alignment with strategic priorities. Strong analytical and problem-solving skills to address challenges in AI integration and policy development through innovative solutions
- Abilities: Ability to develop, implement, enforce policies, and oversee compliance related to AI governance, ethical use, and data management. Ability to align AI initiatives with strategic objectives and operational priorities, anticipating future challenges and opportunities in AI and data management. Ability to thrive in a dynamic and fast-paced environment, managing multiple priorities and adapting to evolving mission needs. Adept at providing executive leadership and guidance for AI programs and policy initiatives for informed decisions that balance innovation, compliance, and mission needs.

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: CCMDS-DoW-FRCWP-26-009

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – CCMDS-DoW-FRCWP-26-009

Host Organization

Name: U.S. Indo-Pacific Command (USINDOPACOM)

Division: J6 - Command, Control, Communications and Cyber Directorate

Mission: USINDOPACOM J6 provides theater assured Command, Control, Communications, Computers and Cyber (C4/Cyber) capabilities enabling USINDOPACOM decision dominance and improved theater posture to deter aggression, prevent and respond to crisis, and if necessary, conduct Joint and Combined operations to prevail in conflict.

Vision: USINDOPACOM J6 plans, synchronizes, and integrates Command, Control, Communications, Computers and Cyber (C4/Cyber) efforts across the theater to engineer, install, operate, maintain, and defend network and data-centric resources with and through our U.S. Alliances and Partnerships--out pacing the threat and enabling the employment of advanced all-domain combat power.

Rotation Opportunity

Title: INDOPACOM J6 - C4/Cyber mission enabler

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Intelligence (Cyberspace) -Technical Support Specialist (411)
- Intelligence (Cyberspace) - Knowledge Manager (431)
- Cybersecurity - Control Systems Security Specialist (462)
- Cybersecurity - Cyber Defense Analyst (511)
- Cybersecurity - Cyber Defense Infrastructure Support Specialist (521)
- Cybersecurity - Cyber Defense Incident Responder (531)
- Cybersecurity - Vulnerability Assessment Analyst (541)

- Cybersecurity - Authorizing Official/Designated Representative (611)
- Cybersecurity - Security Control Assessor (612)
- Cybersecurity - Information Systems Security Manager (722)
- Cybersecurity - COMSEC Manager (723)
- Cyberspace Enablers - Privacy Compliance Manager (732)
- Cyberspace Enablers - Program Manager (801)
- Cyberspace Enablers - IT Project Manager (802)
- Cyberspace Enablers - IT Program Auditor (805)
- Cyberspace Enablers - Executive Cyber Leader (901)

Location: CAMP H.M. Smith (Aeia, Hawaii)

Work Schedule: Monday – Friday, 07:30 – 16:30 (8 hours/day, 40 hours/week)

Travel Requirements: Not required

Duration: 6-12 months

Description: This rotational opportunity provides participants with direct exposure to the J6 Directorate's C4 (Command, Control, Communications, & Computers) and Cyber environment. The participant will support one of the six J6 divisions, contributing to mission-critical tasks and helping to fill identified organizational gaps. This role is designed to be flexible. While specific duties will be tailored to the participant's unique skills and development goals, general responsibilities will include:

- Analyzing C4/Cyber challenges and contributing to innovative solutions.
- Supporting directorate-level projects, policy development, or operational planning.
- Collaborating with internal and external stakeholders to advance J6 objectives.
- Assisting in the management, security, or enhancement of vital communications and information systems.

This assignment offers a unique opportunity to gain hands-on experience in a dynamic joint environment while directly supporting key operational objectives.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Participants will be selected based on their potential to contribute to the J6 mission and their capacity for growth. The ideal candidate will possess a foundational set of the following knowledge, skills, and abilities (KSAs). Specific requirements may be adjusted based on the hosting J6 division and the participant's developmental goals.

Core Competencies

Analytical and Critical Thinking:

- Demonstrated ability to analyze complex problems, identify root causes, and recommend viable solutions.
- Experience in researching, interpreting, and applying technical or policy documentation.
- A proactive, self-motivated approach to identifying and managing tasks.

Communication and Collaboration:

- Strong written and verbal communication skills, with the ability to convey technical concepts to diverse audiences.
- Proven ability to work effectively in a team-oriented, collaborative environment.
- Excellent interpersonal skills and experience building relationships with internal and external partners.

General Technical Aptitude:

- A foundational understanding of IT principles, network fundamentals, cybersecurity concepts, or C4 systems.
- Familiarity with information management, data analysis, or project management processes.
- Adaptability and a strong willingness to learn new technologies, systems, and procedures in a dynamic environment.

Desired Number of Participants: 10

Security Clearance Requirement: Top Secret

Special Requirements/Other: Funding for travel or relocation is not available for this opportunity. Therefore, preference will be given to candidates located on the island of Oahu.

Back to Top

Opportunity Number: DAF-DoW-CITEP-26-010

Anticipated Start Date: August 10, 2026

Apply Here: **Cyber Rotation Programs Application – DAF-DoW-CITEP-26-010**

Host Organization

Name: U.S Air Force - Air Force Operational Test & Evaluation Center (AFOTEC)

Division: Communications & Information Directorate (A6)

Mission: AFOTEC is the Air Force independent test agency responsible for testing, under operationally realistic conditions, new systems being developed for Air Force and multi-service use. The AFOTEC mission is to inform the warfighter through operational test.

Vision: The AFOTEC vision is to be the "Leader of the Test Enterprise – Accelerating Change."

Rotation Opportunity

Title: IT Project Manager – Digital Transformation & Cybersecurity

DoW Cyber Workforce Framework (DCWF) Work Role Code(s): Cyberspace Enablers - IT Project Manager (802)

Location: Kirtland Air Force Base (Albuquerque, New Mexico)

Work Schedule: Day shift hours, office environment. 5 days per week on-site, with potential for telework 1 day a week.

Travel Requirements: Yes

Duration: 12 months

Description: The IT Project Manager will accelerate AFOTEC's digital transformation through strategic management focused on integrating advanced technologies into the AFOTEC baseline and improving the AFOTEC cybersecurity posture. The participant's projects will directly contribute to reduced data analysis time, improved delivery and interpretation of test results, and more efficient test cycles, leading to faster, more informed decision for the warfighter. Key project areas will include cloud migration and infrastructure modernization, data analytics enhancements, network transitions and security upgrades, and supporting Artificial Intelligence (AI) implementation initiatives. Responsibilities include developing project plans, managing and allocating resources, tracking progress, managing risk, and fostering stakeholder buy-in. The Project Manager will collaborate with AFOTEC stakeholders and external partners to deliver solutions.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of project management principles and techniques.

- Knowledge of resource management principles and techniques.
- Knowledge of change management principles and techniques.
- Knowledge of risk management processes and techniques.
- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of IT architectural concepts and frameworks.
- Knowledge of cloud computing, including deployment methods and service models (e.g. SaaS, IaaS, PaaS).
- Knowledge of data migration methods and data security.
- Knowledge of IT procurement requirements and processes.
- Knowledge of cybersecurity principles.
- Knowledge of requirements for operating within a classified environment.

- Skill in planning, organizing and managing IT projects from cradle to grave.
- Skill in identifying and mitigating project risks.
- Skill in understanding and communicating technical information to diverse audiences.
- Skill in stakeholder management.

- Ability to analyze complex IT problems, assess risks, and develop solutions.
- Ability to align IT projects with organizational goals.
- Ability to think critically about security risks and vulnerabilities.
- Ability to balance security requirements with operational needs.
- Ability to anticipate future trends/challenges in cybersecurity and the IT landscape.
- Ability to understand data throughout its lifecycle.
- Ability to lead and motivate project teams.
- Ability to delegate tasks and responsibilities effectively.
- Ability to communicate effectively with technical and non-technical stakeholder.

The selected participant will gain expertise in leading digital transformation initiatives, including cloud migration, data analytics and cybersecurity modernization. The rotation will provide expertise in cross-functional collaboration, deepening the participant's experience working with diverse stakeholders, technical experts, operational personnel and external partners. The participant will gain exposure to emerging military technologies and the test and evaluation lifecycle, with opportunities to apply relevant advanced IT solutions to optimize their effectiveness.

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret/SCI

Special Requirements/Other: The selected candidate will play a critical role in modernizing AFOTEC's processes and delivering digital transformation across the Center. A proactive approach to problem-solving, strong communication skills, a "can do" attitude, and the ability to adapt/learn quickly are essential. Experience with cloud computing environments (Azure, AWS, CloudOne) and project management tools (MS Project, Jira) is highly desired. This is a rare opportunity to shape the future of operational test by driving digital transformation projects to success, directly contributing to superior warfighting capabilities.

Back to Top

Opportunity Number: DAF-DoW-CITEP-26-011

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-CITEP-26-011

Host Organization

Name: Air Force Operational Test & Evaluation Center (AFOTEC)

Division: Directorate of Intelligence, Analyses, and Assessments (AFOTEC/A2/9)

Mission: Inform the Warfighter and Acquisition Through Operational Test

Vision: Leader of the Test Enterprise – Accelerating Change

Rotation Opportunity

Title: AI Digital Transformation Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623)
- Data/AI - Data Architect (653)
- Data/AI - AI Adoption Specialist (753)
- Data/AI - AI Innovation Leader (902)

Location: Kirtland Air Force Base (Albuquerque, New Mexico)

Work Schedule: 5 days/week, on-site

Travel Requirements: Not required

Duration: 6-12 months as allowable by the lending organization

Description: The participant will serve as a key technical expert within AFOTEC's AI Center of Excellence, driving the Center's enterprise-wide digital transformation. The core mission is to help build and integrate a portfolio of AI-powered tools to replace labor-intensive, document-centric workflows with an automated, data-driven Digital Test Ecosystem .

Key responsibilities will include:

- Executing the AFOTEC AI Modernization Strategy: Assist in the phased "Crawl, Walk, Run" implementation of specialized AI tools for measures development, automated classification, and documentation review.
- Building the Digital Backbone: Contribute to the deployment and integration of a foundational workflow platform (e.g., eDaptive Automate) that connects disparate data sources and automates the end-to-end T&E lifecycle.
- Developing AI-Powered Capabilities: Support the development of specific AI applications, such as a natural language search capability (RAG) for the corporate knowledge repository, automated data ingestion pipelines, and model-based document generation from MBSE tools.
- Enabling the Digital Thread: Work with test teams to create and validate the digital link from system requirements (ICDs/CDDs) through test design, data collection, and final reporting, ensuring full traceability and defensibility of findings.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: This rotation offers a unique opportunity to architect and implement an enterprise-level AI solution from the ground up, providing deep, practical experience at the intersection of AI/ML, data engineering, and Department of War (DoW) operational test.

The participant will gain expertise in:

- Enterprise AI Strategy & Implementation: Translating high-level strategy into executable technical pilots and phased rollouts within a government organization.
- AI/ML Application in T&E: Applying Natural Language Processing (NLP), Retrieval Augmented Generation (RAG), and machine learning models to solve real-world problems in requirements analysis, test design optimization, and automated reporting.
- Data Architecture & Engineering: Designing and implementing a centralized T&E knowledge repository, building automated data ingestion pipelines, and establishing data governance standards for a complex enterprise.

- Digital Transformation & Workflow Automation: Integrating COTS/GOTS AI tools into a unified platform to automate complex business processes, including document generation, staffing, and compliance enforcement.
- DoW Acquisition & T&E Domain Knowledge: Gaining a comprehensive understanding of the operational test lifecycle, from initial test design to final reporting, and how AI can accelerate the delivery of capabilities to the warfighter across different acquisition pathways (MTA, SWP, MCA).

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: Seeking a proactive, hands-on technical expert with a proven track record of applying AI and data engineering to solve complex enterprise problems. The ideal candidate will be a creative problem-solver capable of bridging the gap between high-level strategy and practical implementation.

Required Experience:

- Demonstrated experience designing, building, or integrating AI/ML solutions, particularly with NLP, semantic search (RAG), and automated workflow tools
- Proficiency with data architecture, including designing and implementing data pipelines, knowledge repositories, and data governance frameworks.
- Experience with cloud computing platforms (e.g., AWS, Azure) and deploying applications within secure government environments (e.g., Cloud One, Platform One)
- Familiarity with DevSecOps principles and integrating tools via APIs to create a cohesive digital ecosystem.

Desired Experience:

- Experience with Model-Based Systems Engineering (MBSE) tools (e.g., Cameo) and linking models to automated documentation.
- Knowledge of DoW data standards, security classification guidelines (SCGs), and the Risk Management Framework (RMF) process.
- Familiarity with the Test & Evaluation (T&E) or defense acquisition lifecycle.

This is a unique opportunity to join AFOTEC at the very beginning of its enterprise digital transformation. The rotational participant will not be a small cog in a large machine; they will be a central player in shaping the future of Test & Evaluation for the Department of the Air Force. Working directly with AFOTEC's Chief Data and AI Officer, the participant will help execute a funded, multi-year AI Modernization Strategy. They will have the chance to influence technology selection, architect core systems, and

demonstrate tangible value by automating processes for test teams across four geographically separated Detachments. This role offers the rare chance to build a legacy system and gain unparalleled experience in deploying enterprise-scale AI within a critical DoW mission area.

Back to Top

Opportunity Number: DAF-DoW-CITEP-26-012

Anticipated Start Date: August 3, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-CITEP-26-012

Host Organization

Name: Air Force Operational Test & Evaluation Center (AFOTEC)

Division: Air Force Operational Test and Evaluation Center Detachment 6

Mission: Conduct realistic and objective operational testing and evaluation of space, cyber, and intelligence systems to ensure they are effective, suitable, and mission-ready for the warfighter.

Vision: To enhance the management and exploitation of data to increase the effectiveness and timeliness of operational test and evaluation for the War Department.

Rotation Opportunity

Title: Data Subject Matter Expert

DoW Cyber Workforce Framework (DCWF) Work Role Code(s): Data/AI - Data Architect (653)

Location: Nellis Air Force Base (Las Vegas, NV)

Work Schedule: Due to the sensitive nature of the work to be performed, the work schedule will primarily be Monday through Friday during the day. There are opportunities to work hybrid schedules on a limited bases with the Chief Data and Artificial Office (CDAO) approval.

Travel Requirements: Travel is required

Duration: 12 months

Description: This rotation provides the opportunity to work with a relatively new CDAO function within Det 6 charged with bringing innovation to the Department of War fighter operational test and evaluation community. Individual will work with the CDAO Team in the areas of data management, IT architecture, data engineering, requirements management and integration of cloud architecture and AI/ML capabilities.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Individual should have the ability to excel in and agile environment with minimal direction. They should be able to collaborate both within their assigned team as well with external teams within Det 6 and across the Joint Force. The individual should have knowledge, skills, and abilities in the areas of data modeling, matching appropriate database technology with types of data, Extract/Transform/Load design, data governance/security, big data technologies, data lake house (lake & warehouse) design/management, metadata management, and the software development lifecycle. Additional required skills include problem-solving, excellent communications, leadership, project/program management, strategic/critical thinking, and attention to detail.

Desired Number of Participants: 1

Security Clearance Requirement: TS/SCI with required SAP read-ins

Special Requirements/Other: N/A

Back to Top

Opportunity Number: J1-DoW-FRCWP-26-013

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – J1-DoW-FRCWP-26-013

Host Organization

Name: Joint Chiefs of Staff - Directorate for Manpower and Personnel (J-1)

Division: Personnel Readiness Division (PRD)

Mission: Provide the Chairman, Joint Chiefs of Staff, consistently outstanding manpower and personnel advice and support to ensure maximum readiness and sustainability of the total force.

Vision: Foster highly effective communication, cooperation and collaboration between the J1, Joint Staff directorates, Office of the Secretary of Defense (OSD), Services, and Combatant Commands to develop globally integrated solutions to manpower and personnel challenges.

Rotation Opportunity

Title: Personnel Accountability/Personnel Strength Reporting Data Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - Data Analyst (422)
- Data/AI - Data Architect (653)
- Data/AI - Data Officer (903)

Location: Pentagon (Arlington, VA)

Work Schedule: On-site, full 40-hour week. Situational tele-work as approved and coordinated with the supervisor.

Travel Requirements: Travel is required

Duration: 12 months

Description: Joint Staff J-1 requires a data analyst/architect/officer to assist in the development to establish a unified, automated, and real-time Personnel Accountability / Personnel Strength Reporting Framework (PSRF) that ensures accurate and standardized reporting and accountability of all Joint Force personnel across Combatant Commands. This framework eliminates fragmented processes, integrate existing systems, and provide a Common Operating Picture (COP) to enhance operational readiness, decision-making, and crisis response. Success is achieved when the Joint Force has a fully operational PSRF that delivers timely, accurate, and actionable personnel data, enabling seamless coordination and support for both steady-state and contingency operations.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Data analyst, data engineering, data visualization, common operational picture (COP development)

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret/SCI

Special Requirements/Other: N/A

Back to Top

Opportunity Number: TRMC-DoW-FRCWP-26-014

Anticipated Start Date: August 15, 2026

Apply Here: Cyber Rotation Programs Application – TRMC-DoW-FRCWP-26-014

Host Organization

Name: Test Resource Management Center (TRMC)

Division: National Cyber Range Complex (NCRC)

Mission:
TRMC Mission: Ensure Readiness of the Department of War (DoW) Test and Evaluation (T&E) Infrastructure

NCRC Mission: The NCRC plans, coordinates, and conducts robust, full-spectrum cyber test and evaluation, workforce training, and mission rehearsal events for the DoW cyber test, training, experimentation, and acquisition communities to enhance the resilience of our systems and the effectiveness of our offensive capabilities.

Vision:

NCRC Vision: Continued evolution to provide the best-of-breed cyber range facilities, tools, and expertise to test and evaluate all acquisition, research and development, and science and technology programs throughout their lifecycles and to meet the most challenging cyber training and mission rehearsal requirements.

Rotation Opportunity

Title: National Cyber Range Complex - Cyber Range Program Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyber Operations Planner (332)
- Cyberspace Effects - Cyberspace Capability Developer (341)

- Data/AI - Data Scientist (423)
- Data/AI - AI/ML Specialist (623)
- Software Engineering - Software Test & Evaluation Specialist (673)
- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)

Locations:

- Orlando, FL
- Patuxent River, MD
- Charleston, SC

Work Schedule: On-site (opportunity for remote work)

Travel Requirements: It depends on OPTEMPO and event schedule

Duration: 12 months

Description: This position is responsible for coordinating, managing, and executing technical and enterprise activities across four key areas: Cyber Event Operations, Range Engineering, Cybersecurity, and Cyber Workforce Development. This position could require:

- Supporting end-to-end operational readiness and execution of cyber test, training, and exercise events within the cyber range environment.
- Supporting the Enterprise Leadership in preparing presentations, briefings, and reports for senior leadership and external stakeholders.
- Translating complex operational and training needs into clear, actionable requirements for the engineering team.
- Assisting in the design, development, and maintenance of cyber training curricula, courses, and hands-on scenarios aligned with industry standards.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Cyber Range Event Planning Experience
- Cyber Range Architecture and Operations
- Curriculum Development Models
- Application of cybersecurity evaluations processes
- Enterprise Level Program Management

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: There are a lot of mission areas within the NCRC enterprise. The goal of this rotation is to expose the participant to multiple functions within the organization - technical and programmatic.

Back to Top

Opportunity Number: DAF-DoW-CITEP-26-015

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-CITEP-26-015

Host Organization

Name: U.S Air Force - 333d Training Squadron

Division: TRR – Curriculum development

Mission: Forging agile communications and cyber forces through world-class training to project power anytime, anywhere.

Vision: To be the world's greatest training organization, unleashing the full potential of tomorrow's operators...the Mad Duck way.

Rotation Opportunity

Title: Industry Cyber Training Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyberspace Operator (322)
- Cyberspace Effects - Cyber Operations Planner (332)
- Cyberspace Enablers - Cyber Instructional Curriculum Developer (711)
- Cyberspace Enablers - Cyber Instructor (712)
- Data/AI - AI Adoption Specialist (753)
- Cyberspace Enablers - IT Project Manager (802)
- Data/AI - AI Innovation Leader (902)

Location: Gulf coast, white sand beaches in Biloxi, MS

Work Schedule: Normal schedule - fully on site 5 days a week 8 hours a day. Could be remote if bring expert technical skills for curriculum development.

Travel Requirements: Travel not required

Duration: 3 – 12 months

Description: The 333d Training Squadron is seeking a visionary industry professional to serve as a forward-leaning Curriculum Developer, responsible for pioneering the next generation of training programs for cyber professionals. This critical role will architect and transition our instructional approach towards a robust Competency-Based Learning (CBL) model, moving beyond traditional knowledge transfer to focus on measurable skill attainment and real-world application.

Leveraging deep, hands-on industry expertise, the selected individual will design, develop, and implement truly cutting-edge educational content alongside training curriculum developers. This development is crucial for preparing our cyber force for future instruction methodologies, seamless AI integration into cyber operations, and strategic engagement against near-peer adversaries. The goal is to ensure our foundational and advanced courses are not only robust and relevant today, but are also future-proofed, delivering the essential skills and adaptability required for evolving military operational needs and the dynamic cyber battlespace.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: We seek an industry professional with willingness to architect and implement Competency-Based Learning (CBL) models, developing next-generation, future-proofed cyber training programs. This requires deep, hands-on technical proficiency in advanced cyber operations, networking, and systems manipulation, emphasizing AI/ML integration in both offensive and defensive contexts. Candidates must possess a forward-looking grasp of any of the following: strategic cyber operations, operational planning, and tactical hands-on training to develop leaders within the air force. A visionary mindset with proven project management skills is essential for identifying, developing, and deploying innovative educational solutions that enhance instruction and accelerate skill acquisition.

Desired Number of Participants: 2-4

Security Clearance Requirement: Not required

Special Requirements/Other: This rotation offers a unique and profound opportunity to directly shape the next generation of cyber leaders, ensuring the security of our nation and way of life. You will leverage your industry expertise to develop cutting-edge, competency-based

curriculum, translating your passion for cyber into training that directly contributes to national security and operational effectiveness. Beyond curriculum development, this is a unique two-way exchange: you will mentor aspiring cyber officers and operators, while gaining invaluable insights from those actively serving on the front lines of cyber warfare. Your goal will be to design immersive, activity-based learning environments that instill the critical hands-on skills necessary to confront complex, real-world cyber challenges.

Back to Top

Opportunity Number: DCAA-DoW-FRCWP-26-016

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DCAA-DoW-FRCWP-26-016

Host Organization

Name: Defense Contract Audit Agency (DCAA)

Division: DCAA Office of Chief Information Officer

Mission: DCAA delivers contract audit and advisory services that exceed our customers' expectations to promote timely acquisition decisions and maximize buying power, so DoW has the necessary capabilities to deter current and emerging threats.

Vision: As the premier leader in DoW contract audit and advisory services, we deliver unparalleled value, agile solutions, and data driven insights in support of our nation's defense needs.

Rotation Opportunity

Title: Information Systems Security Manager (CSSP)

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Cyber Defense Infrastructure Support Specialist (521)
- Cybersecurity - Information Systems Security Developer (631)
- Cybersecurity - Information Systems Security Manager (722)

Location: Irving, TX and Fort Belvoir, VA

Work Schedule: On-site

Travel Requirements: Minimal travel required

Duration: 9 months

Description: This rotational opportunity provides participants with hands-on experience in critical information security and cybersecurity functions, including managing and enhancing programs, conducting security assessments, and supporting the organization's IT infrastructure and compliance with national.

Key responsibilities include:

- Information Security Management:
  - Develop and implement security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of systems, networks, and data.
  - Conduct risk and vulnerability assessments, security evaluations, and audits to identify and mitigate risks.
  - Promote security awareness and ensure alignment with organizational goals.

- Cybersecurity Program/Project Management:
  - Define and manage cybersecurity initiatives, including strategic planning, resource allocation, and policy enforcement.
  - Provide oversight and coordination to ensure program objectives are met effectively.

- Information Security Auditing:
  - Validate and oversee documentation and accreditation processes for IT systems.
  - Assess threats and vulnerabilities, ensuring compliance with security standards and recommending mitigation strategies.

- Incident Response and Forensic Analysis:
  - Facilitate evidence gathering and analysis for cybersecurity incidents.
  - Implement corrective actions to address security events and ensure system resilience.

- Additional Responsibilities:
  - Participate in network and systems design to integrate security measures.
  - Develop contingency plans and disaster recovery procedures.
  - Perform occasional travel and other duties as assigned.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Participants in this rotational opportunity are expected to gain the following knowledge, skills, and expertise:

- Advanced Cybersecurity Knowledge:
  - Understanding of information security principles, concepts, and methodologies.
  - Expertise in risk and vulnerability assessment, incident response, and forensic analysis.
  - Familiarity with cybersecurity tools, techniques, and frameworks.

- Policy and Compliance Expertise:
  - Knowledge of security policies, procedures, and compliance standards, including Department of War (DoW) and agency-specific requirements.
  - Ability to develop and implement security programs aligned with organizational goals and national security standards.

- Technical Skills:
  - Proficiency in designing and implementing security controls for systems and networks.
  - Hands-on experience with cloud computing environments, including risk management and incident response strategies.
  - Skills in conducting security evaluations, audits, and accreditation processes.

- Project and Program Management:
  - Ability to define, manage, and oversee cybersecurity programs or projects.
  - Strategic planning and resource allocation skills to support program objectives.
  - Workforce development and budget forecasting expertise.

- Problem-Solving and Analytical Abilities:
  - Capability to analyze complex IT issues and develop innovative solutions.
  - Skills in identifying and mitigating security threats and vulnerabilities.

- Communication and Collaboration:
  - Strong ability to promote security awareness and influence stakeholders to adopt security measures.
  - Experience in coordinating with cross-functional teams and external agencies.

This opportunity is designed to equip participants with the technical expertise, strategic thinking, and leadership skills necessary to excel in cybersecurity and information

security roles, while fostering professional growth and adaptability in a dynamic IT environment.

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DCAA-DoW-CITEP-26-017

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DCAA-DoW-CITEP-26-017

Host Organization

Name: Defense Contract Audit Agency (DCAA)

Division: Chief Information Officer (CIO)

Mission: DCAA delivers contract audit and advisory services that exceed our customers' expectations to promote timely acquisition decisions and maximize buying power, so DoD has the necessary capabilities to deter current and emerging threats.

Vision: As the premier leader in DoD contract audit and advisory services, we deliver unparalleled value, agile solutions, and data driven insights in support of our nation's defense needs.

Rotation Opportunity

Title: Data Scientist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623)
- Data/AI - Data Architect (653)
- Data/AI - Data Officer (903)
- Data/AI - Data Operations Specialist (624)

- Data/AI - Data Scientist (423)

Location: Fort Belvoir, VA

Work Schedule: On-site

Travel Requirements: Minimal

Duration: 9 months

Description: This rotational opportunity provides participants with hands-on experience in implementing the agency's data strategy, shaping governance frameworks, and contributing to future-focused data management practices, including drafting policies and procedures for utilizing the new data lakehouse. Participants will play a key role in supporting data governance, analytics, and AI initiatives while collaborating across the agency to ensure alignment with strategic goals.

Key responsibilities include:

1. Data Governance and Management:
    a. Develop and implement foundational policies, standards, and procedures to ensure data quality, security, access, and sharing.
    b. Establish and maintain a data asset inventory, catalog, and business glossary to improve transparency and understanding.
    c. Contribute to master data management, reference data management, and metadata management efforts to create a single source of truth for critical data elements.
    d. Support the design and execution of a data quality program, including defining metrics, remediating issues, and reporting on data health.
2. Analytics and AI Governance:
    a. Assist in developing frameworks for the ethical and effective use of analytics, AI, and Machine Learning (ML) models, aligning with DoD Responsible AI principles.
    b. Collaborate on creating an MLOps playbook to standardize the lifecycle of AI/ML models, emphasizing Explainable AI (XAI).
    c. Define policies for analytics development to ensure centralized, authoritative sources for strategic analytics and prevent model proliferation.
    d. Support decision frameworks for executing data workloads across internal and enterprise platforms based on mission requirements.
3. Policy Development for Data Lakehouse Utilization:
    a. Draft policies and practices for the effective use of the agency's new data lakehouse, ensuring alignment with strategic data management goals.

    b. Assist in architecting future data management practices to optimize the use of the data lakehouse for analytics, reporting, and AI/ML workloads.
4. Program Leadership and Stakeholder Engagement:
    a. Collaborate with agency directorates to translate governance requirements into actionable guidance.
    b. Promote a data-aware culture through training programs, strategic communication, and stakeholder education.
    c. Monitor industry trends and government mandates to ensure the governance program remains modern and effective.
    d. This opportunity is designed to be adaptable to individual participants' skills and development goals, ensuring a tailored and impactful experience.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

Participants in this rotational opportunity are expected to gain the following:

- Data Governance Expertise:
    - Knowledge of foundational policies, standards, and procedures for data quality, security, access, and sharing.
    - Skills in managing data assets, including creating inventories, catalogs, and business glossaries to improve transparency and understanding.
- Advanced Data Management Skills:
    - Expertise in master data management, reference data management, and metadata management to establish a single source of truth for critical data elements.
    - Ability to design and execute data quality programs, including defining metrics, remediating issues, and reporting on data health.
- Analytics and AI Governance Knowledge:
    - Understanding of ethical and effective use of analytics, AI, and Machine Learning (ML) models, including alignment with DoD Responsible AI principles.
      Skills in developing MLOps frameworks for AI/ML lifecycle management, emphasizing Explainable AI (XAI).
    - Ability to define policies for analytics development and manage centralized, authoritative sources for strategic analytics.
- Policy Development and Implementation:
    - Expertise in drafting policies and practices for utilizing a data lakehouse and architecting future data management practices.
    - Knowledge of decision frameworks for executing data workloads across internal and enterprise platforms.
- Program Leadership and Collaboration:

    - Skills in stakeholder engagement, translating governance requirements into actionable guidance, and promoting a data-aware culture.
    - Ability to monitor industry trends and government mandates to ensure governance programs remain modern and effective.
- This opportunity equips participants with technical expertise, strategic thinking, and leadership skills necessary to excel in data governance, analytics, and AI roles, while fostering professional growth and adaptability in a dynamic environment.

Desired Number of Participants: 1

Security Clearance Requirement: Public Trust

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DCMA-DoW-FRCWP-26-018

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DCMA-DoW-FRCWP-26-018

Host Organization

Name: Defense Contract Management Agency (DCMA)

Division: Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

Mission: Support the warfighter by assessing the Defense Industrial Base compliance in the protection of DoD Controlled Unclassified Information, ensuring contractors implement appropriate cybersecurity requirements, in support of acquisition decision making.

Vision: Security-focused, highly trained cybersecurity professionals providing comprehensive and repeatable assessments for risk-based decision making.

Rotation Opportunity

Title: Cybersecurity Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Security Control Assessor (612)

Location: Mobile work opportunity with up to 50% travel

Work Schedule: Maxi-Flex schedule

Travel Requirements: Yes

Duration: 12 Months

Description: The opportunity involves conducting comprehensive cybersecurity assessments to evaluate contractor compliance with established regulations and standards, including those outlined by NIST, DOD, and DCMA. The role requires reviewing contractor unclassified information systems, assessing information security policies, programs, and physical controls, and ensuring alignment with cybersecurity requirements. The incumbent will plan, coordinate, and facilitate multiple assessments simultaneously, tailoring each to the unique cybersecurity posture of the contractor. Responsibilities include interpreting high-level instructions, monitoring evolving cybersecurity policies, and staying informed about emerging threats and attack vectors. Additionally, the role entails formally representing the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) during assessments, articulating findings, responding to inquiries, and maintaining assessment data in a DOD-level database for use by various stakeholders. Operating within a geographically dispersed team, the incumbent may serve as the lead assessor, providing leadership during pre-assessment activities, daily operations, and post-assessment documentation.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: In this role, individuals will learn how to plan, coordinate, analyze, and report compliance related to DFARS 252.204-7012. They will develop proficiency in applying project management concepts, methods, and practices, including effective project organization, communication, and documentation. They will gain knowledge of IT vulnerabilities and learn to create standards and methodologies for identifying and reporting them. A foundational understanding of information architecture, governance, and IT strategy will be acquired. Participants will also learn about cybersecurity requirements, including NIST standards and DCMA policies, to manage contractor compliance reviews and corrective actions. Additionally, they will build the ability to assess systems security, requirements, and processes to address complex technical scenarios and ensure proper evaluation of new developments.

Desired Number of Participants: 1

Security Clearance Requirement: Secret

Special Requirements/Other: Must have government travel card. DoD to DoD only for this program.

Back to Top

Opportunity Number: DoN-DoW-FRCWP-26-019

Anticipated Start Date: August 31, 2026

Apply Here: Cyber Rotation Programs Application – DoN-DoW-FRCWP-26-019

Host Organization

Name: U.S. Navy

Division: Office of the Department of Navy Principal Cyber Advisor

Mission: Reestablish warfighting advantage in and through cyberspace. The Department of Navy Principal Cyber Advisor (DON PCA) is the senior advisor to Department of Navy leadership on all cyber matters.

Vision: To deliver warfighting advantage to the Sailors and Marines we serve by leading the integration of the DON's cyber activities and investments.

- SECURE defense critical infrastructure
- SURVIVE cyber attacks afloat
- STRIKE with a ready cyber mission force

Rotation Opportunity

Title: Cyber Policy Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)

Location: Pentagon

Work Schedule: Full time, in person.

Travel Requirements: No

Duration: 6-12 months

Description: As a Cyber Policy Analyst in the PCA office, you will:

- Evaluate, research, and develop cyber policies. Provide informed recommendations and insights guiding and influencing the development of Department of Navy (DON) and Department of War (DoW) cyber policies and strategies, strengthening overall cyber posture.
- Consistently analyze cyber posture and policy data to identify weaknesses, patterns, and trends. Communicate findings to relevant stakeholders and senior leaders.
- Support DON PCA strategic engagements to effectively convey program objectives, department-wide initiatives, and key outcomes to internal and external stakeholders.
- Support legislative affairs work by tracking relevant developments, contributing to policy analysis, and aiding in engagement with oversight and legislative bodies.
- Contribute to DON and DoW cyber working groups completing statutory-required reporting.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: This is a policy-focused position that requires strong analytical skills, clear communication, and the ability to engage across the Department of War, the Department of Navy, and external partners.

- Background in cyber OR policy OR legislative affairs
- Strong written and verbal communication skills

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret / Secret

Special Requirements/Other:

- Desire Top Secret clearance, Secret clearance required at a minimum
- Desire GS-11 equivalent or above
- Also open to a rotation from federal agencies outside of DoW

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-021

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-021

Host Organization

Name: Defense Information Systems Agency - DISA Europe (No. 001)

Division: Defensive Cyber Operations Branch

Mission: DISA Europe provides, operates, maintains, and defends the DISN to assure DODIN Enterprise Solutions and capabilities enabling joint warfighting functions throughout all domains supporting Combatant Commands, their Components, Allies, and mission partners within the European Theater.

Vision: DISA Europe provides a secure, data-centric, coalition enterprise that enables access to critical information at the speed of decision for the warfighter and mission partners.

Rotation Opportunity

Title: DISA Europe Fellowship

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623)

Location: Patch Barracks, USAG Stuttgart, Germany

Work Schedule: Can be fully remote but on-site is preferred.

Travel Requirements: Yes

Duration: 6-12 months

Description: DISA Europe is seeking expertise in AI/ML to support Defensive Cyberspace Operations (DCO) by moving beyond basic automation or chatbot solutions. The focus is on building and leveraging complex models that can process and analyze large volumes of network traffic to detect anomalies and potential threats, while also exploring innovative ways to incorporate AI/ML into business and mission practices. This role requires applying advanced data science techniques to strengthen cyber defense, improve decision-making, and drive the integration of emerging technologies into DCO operations.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Expertise in AI/ML with a focus on supervised, unsupervised, and anomaly detection methods, along with a strong background in network traffic analysis, cybersecurity, and DCO. Candidates should be proficient in Python, R, and common ML frameworks such as TensorFlow, PyTorch, and Scikit-learn, with the ability to design, train, and deploy scalable models on large datasets. Experience in data engineering and analyzing complex network data is essential, as is the ability to integrate AI/ML solutions into mission and business workflows. Success in this role requires effectively translating mission needs into technical solutions and bringing an innovative mindset to a rapidly evolving cyber and AI environment.

Desired Number of Participants:1-2

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-022

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-022

Host Organization

Name: Defense Information Systems Agency - DISA Europe (No. 002)

Division: Defensive Cyber Operations Branch

Mission: DISA Europe provides, operates, maintains, and defends the DISN to assure DODIN Enterprise Solutions and capabilities enabling joint warfighting functions throughout all domains supporting Combatant Commands, their Components, Allies, and mission partners within the European Theater.

Vision: DISA Europe provides a secure, data-centric, coalition enterprise that enables access to critical information at the speed of decision for the warfighter and mission partners.

Rotation Opportunity

Title: DISA Europe Fellowship

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Intelligence (Cyberspace) - All-Source Analyst (111)

Location: Patch Barracks, USAG Stuttgart, Germany

Work Schedule: Can be fully remote but on-site is preferred.

Travel Requirements: Yes

Duration: 6 months

Description: All-Source Analyst able to support cyberspace operations by delivering timely, actionable intelligence tailored to our mission and network terrain. The focus is on fusing open-source, closed-source, and classified intelligence to provide real-time threat analysis and identify indications of compromise (IOCs) relevant to our area of operations. This role requires the ability to sift through diverse data streams, correlate threat activity, and translate intelligence into operational insights that sharpen and inform deliberate defense measures. The ideal candidate will anticipate emerging threats, enable proactive defensive cyberspace operations, and ensure our defensive posture remains aligned to both adversary capabilities and mission priorities.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Seeking an analyst with expertise in all-source intelligence methods, cyber threat actors and TTPs, indications and warnings, and defensive cyberspace operations. Candidates should be skilled at collecting and correlating data from open-source and classified intelligence, producing actionable intelligence, and using analytic frameworks and threat modeling. Strong communication and collaboration across cyber, intelligence, and operations teams is essential, along with the ability to provide real-time threat analysis tailored to our network terrain, identify and track IOCs, anticipate emerging threats, and translate intelligence into operational recommendations in a dynamic cyber environment.

Desired Number of Participants: 1-2

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-023

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-023

Host Organization

Name: Defense Information Systems Agency - DISA Europe (No. 003)

Division: Defensive Cyber Operations Branch

Mission: DISA Europe provides, operates, maintains, and defends DISN to assure DODIN Enterprise Solutions and capabilities enabling joint warfighting functions throughout all domains supporting Combatant Commands, their Components, Allies, and mission partners within the European Theater.

Vision: DISA Europe provides a secure, data-centric, coalition enterprise that enables access to critical information at the speed of decision for the warfighter and mission partners.

Rotation Opportunity

Title: DISA Europe Fellowship

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Software Engineering -Software/Cloud Architect (628)

Location: Patch Barracks, USAG Stuttgart, Germany

Work Schedule: Can be fully remote but on-site is preferred.

Travel Requirements: Yes

Duration: 6 months

Description: A Software/Cloud Architect capable of leading the migration and modernization of our existing sandbox environment into the cloud. This effort will expand enterprise capabilities for tool testing and development while also enabling Continuity of Operations (COOP) through resilient, scalable cloud services. The architect will design and implement secure, flexible cloud-

based solutions that integrate with mission systems, ensure compliance with DoD standards, and provide a robust environment for innovation, experimentation, and operational continuity.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Candidates should have expertise in cloud platforms (AWS, Azure, Google Cloud) and secure, scalable architecture design; experience migrating environments and deploying cloud-native services; and strong proficiency in DevSecOps, containerization, and automation tools. Certifications such as AWS Solutions Architect, Microsoft Azure Architect, or Google Cloud Professional Architect are highly desired, along with DoD 8570/8140 cybersecurity compliance. Success requires the ability to integrate cloud solutions into mission systems, support enterprise tool testing and development, and ensure COOP through resilient cloud capabilities in a dynamic cyber environment.

Desired Number of Participants: 1-2

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-024
Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-024

Host Organization

Name: Defense Information Systems Agency - DISA Europe (No. 004)

Division: Future Operations

Mission: DISA Europe provides, operates, maintains, and defends to assure DoDIN Enterprise Solutions and capabilities while executing unified command and control throughout the full spectrum of operations supporting EUCOM, AFRICOM, and other mission partners.

Vision: N/A

Rotation Opportunity

Title: Change Management Coordinator

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyber Defense Incident Responder (531)
- Technical Support Specialist (411)
- Network Operations Specialist (441)

Location: USAG Stuttgart, Germany (No. 004)

Work Schedule: On-site only

Travel Requirements: No

Duration: 6 months

Description: An opportunity for two (2) GS-12/13 employees to perform duties as a Change Management Coordinator for DISA Europe, Operations Division (EU3), Future Operations (EU35).

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Develop deeper insight and understanding of the unique challenges facing Change Management within the Agency, combatant commands, service components, and mission partners. Gain valuable professional experience from daily interactions with customers, DISA organizations, and international vendors throughout USEUCOM, USAFRICOM, and USCENTCOM AORs.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Applicants with previous or current Change Management experience are highly encouraged to apply. Due to increased mission requirements in support of two active conflicts within theater, key qualifications include expert written and verbal communication skills, proficient knowledge of network operations, and strong decision-making skills.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-025

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-025

Host Organization

Name: Defense Information Systems Agency - DISA Europe (No. 005)

Division: Future Operations

Mission: DISA Europe provides, operates, maintains, and defends to assure DoDIN Enterprise Solutions and capabilities while executing unified command and control throughout the full spectrum of operations supporting EUCOM, AFRICOM, and other mission partners.

Vision: N/A

Rotation Opportunity

Title: Data Scientist or Data Analyst for DISA's first full-time Data Cell

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623)
- Data/AI - Data Analyst (422)
- Data/AI - Data Scientist (423)

Location: USAG Stuttgart, Germany

Work Schedule: In-person only

Travel Requirements: No

Duration: 6 months

Description: An opportunity for two (2) GS-12/13 employees to perform duties as a Data Scientist or Data Analyst for DISA Europe, Operations Division (EU3), Future Operations (EU35).

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Be part of the team leading the Agency-wide push to utilize home-grown tools and emerging technologies in pursuit of data integration for the Agency, combatant commands, service components, and mission partners. Develop deeper insight and understanding of the unique challenges facing data integration in Europe. Gain valuable professional experience from daily interactions with international vendors throughout the USEUCOM, USAFRICOM, and USCENTCOM AORs.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Applicants with data integration or AI experience are highly encouraged to apply. Due to increased mission requirements in support of two active conflicts within theater, key qualifications include expert written and verbal communication skills, proficient knowledge of network operations, and strong decision-making skills.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-026

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-026

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: J5 Plans and Strategy/J53 Plans Integration

Mission: DISA J5 Plans and Strategy Division conducts operational and strategic planning to develop the agency's cyberspace campaign plans and policies, synchronizes specific and broad DISA support capabilities to coordinate enabling capabilities related to support Combatant Commands (CCMDs) campaigns related to command and control (C2) solutions, global infrastructure, telecommunications, cyber operations, and interoperability for information advantage with mission partners.

Vision: To ensure DISA's capabilities are aligned to support CCMD and postured to always execute and be effective.

Rotation Opportunity

Title: Data Analyst, a Data Operation Specialist, or a Strategic Planner/Coordinator

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)
- Data/AI - AI Risk & Ethics Specialist (733)
- Data/AI - Data Analyst (422)
- Data/AI - Data Operations Specialist (624)

Location: Fort George G. Meade, Maryland (No. 006)

Work Schedule: On-site

Travel Requirements: No

Duration: 6 months

Description: An opportunity for multiple individuals to provide planning and analysis in support of work across DISA as a Data Analyst, a Data Operation Specialist, or a Strategic Planner/Coordinator. Seeking (1) person for each role. This detail provides an excellent insight to discover and perform a variety of complex duties/projects, identify guidance or courses of action to inform senior leadership on long-range strategic objectives.

- The selectee(s) must identify issues of organizational importance, and reflect organizational positions in meetings with users, contractors, industry, and mission partners.
- The work involves functioning as a Senior Advisor, Data Analyst, and Planner in their role in support of DISA operations, plans and readiness management. The selectee(s) will engage in planning, organizing, and completing broad and complex analytical studies and initiatives associated with the development and implementation of comprehensive, DISA-wide capabilities.
- The selectee(s) will develop new ways to measure program accomplishments, results, and effectiveness. As such, the incumbent will coordinate efforts and advise Agency officials on feasibility and resource requirements for long-range business and system integration strategies.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of DISA's Next Strategy and other Director level strategic initiatives

- Ability or experience to communicate and collaborate with representatives of the DISA Field Command and Field Offices, J-Directorates, and other agencies.
- Ability to gather, formulate, and develop mission planning requirements in response to agency directives, guidance and/or objectives.
- Ability to brief senior leadership on planning proposals, complex findings, and recommendations.
- Have knowledge about DISA/DCDC planning affiliated Mission Essential Functions (MEF) or Mission Essential Tasks (METs) that support an agency and/or external staff elements that align to current planning efforts.

Desired Number of Participants: 3

Security Clearance Requirement: Top Secret

Special Requirements/Other: Must possess appropriate clearance/access to work in the SCIF.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-27-027

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-027

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: J5 Plans and Strategy/J53 Plans Integration

Mission: DISA J5 Plans and Strategy Division conducts operational and strategic planning to develop the agency's cyberspace campaign plans and policies, supports USCYBERCOM and provides support to the Combatant Commanders in the development of global, theater, and contingency cyberspace plans to meet the agency's commitment to fight and win in cyberspace.

Vision: To ensure DISA's CCMD campaign plans and policies are postured to always execute and be effective.

Rotation Opportunity

Title: Cyber Operations Planner

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyber Operations Planner (332)

Location: Fort George G. Meade, Maryland (No. 007)

Work Schedule: On-site

Travel Requirements: No

Duration: 6 months

Description: An opportunity for multiple GS/GG-12/13 employees to perform the duties as a Cyber Operations Planner for the J5 Plans and Strategy/ J53 Plans Integration Branch. This detail provides an excellent opportunity for professional development within the context of participating in joint and deliberate planning processes in support of Combatant Commands. The selectee will be required to assist J53 with reviewing, updating, and/or developing OPLANs, Campaign, or Support plans to ensure the Agency is prepared to provide global support during campaigning, crisis or conflict. No promotions will be authorized under the DISA Centralized Rotational Program.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of DISA's Next Strategy and other Director level strategic initiatives.
- Ability or experience to communicate and collaborate with representatives of the DISA Combatant Command Field Command and Field Offices, J-Directorates, and other agencies.
- Ability to gather, formulate, and develop mission planning requirements in response to agency directives, guidance and/or objectives.
- Ability to brief senior leadership on planning proposals, complex findings, and recommendations.
- Have knowledge about DISA/DCDC planning affiliated Mission Essential Functions (MEF) or Mission Essential Tasks (METs) that support an agency and/or external staff elements that align to current planning efforts.

Desired Number of Participants: 3

Security Clearance Requirement: Top Secret

Special Requirements/Other: Must possess appropriate clearance/access to work in the SCIF.

Back to Top

Opportunity Number: DAF-DoW-FRCWP-26-028

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-FRCWP-26-028

Host Organization

Name: Department of Air Force - 38th Cyberspace Operations Group

Division: Engineering Squadron - Performance Monitoring - Data Analytics

Mission: Deliver and secure the Air Forces' cyberspace capabilities

Vision: Develop Airmen and harness technology for the U.S. advantage

Rotation Opportunity

Title: Voice System Architect: US Installations in processing to fully VoIP/UC migration - 911 system

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Software Engineering - Systems Security Analyst (461)

Location: Tinker AFB, OK preferred (local site), but flexible to any location.

Work Schedule: N/A

Travel Requirements: Depend on assignments

Duration: 6 months

Description: Familiar with entirely weapon system inventory in technical direction.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Knowledge and experience in real world cyber laws and cyber security principles while implementing and operating weapon systems.

Desired Number of Participants: N/A

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DAF-DoW-FRCWP-26-029

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DAF-DoW-FRCWP-26-029

Host Organization

Name: Department of Air Force - Space Systems Command

Division: Systems Delta 85 - Global Mission Data Dominance

Mission: Create a unified and ubiquitous information ecosystem where mission data flows seamlessly from sensor to effector, empowering Guardians and the joint force with the interoperability and information dominance required to prevail in a contested space domain.

Vision: Deliver a unified data capability to USSF Guardians, integrating data transport, access, and intelligence to ensure timely delivery of trusted information for superior decision-making.

Rotation Opportunity

Title: Data Operations Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)
- Data/AI - Data Architect (653)
- Data/AI - Data Operations Specialist (624)
- Data/AI - Data Officer (903)
- Data/AI - Data Analyst (422)

Location: Peterson Space Force Base

Work Schedule: On site M-F 40hrs

Travel Requirements: No

Duration: 12 months

Description: Contribute to strategic planning by identifying how data is processed, protected, integrated, and disseminated.
Conduct research and review technical artifacts to identify problems and recommend solutions.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Experience with DoW and DAF Data Governance, data sharing, and security protocols.
- Knowledge of advanced multidisciplinary engineering practices, including data science and computer science.
- Ability to apply experimental theories and new developments to solve complex problems.
- Proven ability to conduct research and review technical artifacts.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DoWEA-DoW-CITEP-26-030

Anticipated Start Date: August 3, 2026

Apply Here: Cyber Rotation Programs Application – DoWEA-DoW-CITEP-26-030

Host Organization

Name: Department of War Education Activity (DoWEA)

Division: IT Division

Mission: Educate, Engage, and Empower military-connected students to succeed in a dynamic world.

Vision: Excellence in Education for Every Student, Every Day, Everywhere.

Rotation Opportunity

Title: AI Solutions Architect

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI Adoption Specialist (753)

Location: Alexandria, VA

Work Schedule: Hybrid, on site with the option of telework.

Travel Requirements: No

Duration: 12 months

Description: The AI Solutions Architect leads the design, development, and implementation of enterprise AI capabilities that enhance teaching, learning, and IT operations across DoW Education Activity. The role spans solution architecture, MLOps, data engineering alignment, model governance, and secure deployment within DoD enterprise constraints. The incumbent partners with academic, operational, cybersecurity, privacy, legal, and data governance stakeholders to translate mission needs into reliable, ethical, and compliant AI solutions that scale across regions and schools.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: This position serves as the AI Solutions Architect within the Department of War Education Activity), Office of the CIO (OCIO). The selectee will lead the design, development, and implementation of secure, scalable, and mission-aligned artificial intelligence capabilities that support our global K–12 educational enterprise. They will serve as the agency's technical authority for AI/ML system architecture, solution integration, and responsible AI practices. The selectee must possess expert knowledge of artificial intelligence and machine learning principles, including supervised and unsupervised learning, deep learning, natural language processing, computer vision, model evaluation, and optimization techniques. Knowledge of enterprise IT architecture is required, including microservices, APIs, system integration patterns, cloud computing environments, containerization (e.g., Docker, Kubernetes), and event-driven or service-oriented architectures.

Desired Number of Participants: 1

Security Clearance Requirement: Secret

Special Requirements/Other: DoD Education Activity is actively engaged in systemwide transformation, driven by its Blueprint for Continuous Improvement, which focuses on Student Excellence, School Excellence, Talent Excellence, and Organizational Excellence.
Joining DoD Education Activity—especially in a technology or AI-related role—means contributing directly to modernization efforts that shape the future of teaching, learning, and operational support across a global school system.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-031

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-031

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: Europe Regional Field Command (EU4)

Mission: DISA Europe provides, operates, maintains, and defends the DISN to assure DoDIN Enterprise Solutions and capabilities enabling joint warfighting functions throughout all domains supporting Combatant Commands, their Components, Allies, and mission partners within the European Theater.

Vision: DISA Europe provides a secure, data-centric, coalition enterprise that enables access to critical information at the speed of decision for the warfighter and mission partners.

Rotation Opportunity

Title: Knowledge Operations Manager

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Intelligence (Cyberspace) - Knowledge Manager (431)

Location: USAG Stuttgart-Patch Barracks, DE (No. 008)

Work Schedule: On-site full time.

Travel Requirements: No

Duration: 12 months

Description: Working alongside IT Project Managers, the Knowledge Manager Leads KM internal to DISA Europe that enables collaboration, information reuse, and decision making at all levels of DISA Europe and with USEUCOM and NATO partners. Provides service and project deliverables, coordinated with HQ project managers including site concurrence letters, bill of materials, and requests for information to enable overall project delivery timelines in anticipation of warfighter's requirements

We are seeking a highly motivated Knowledge Manager to champion the capturing, organization, and sharing of critical organizational knowledge. As Knowledge Manager, you'll be responsible for developing and implementing knowledge management strategies, identifying knowledge gaps, creating accessible knowledge repositories, fostering a culture of collaboration, and measuring the impact of knowledge sharing initiatives. You'll curate content, facilitate communities of practice, integrate knowledge into workflows, and ensure knowledge is readily available to empower employees and drive organizational performance. The ideal candidate possesses strong communication, project management, and analytical skills, with a proven ability to cultivate a knowledge-sharing environment and optimize organizational efficiency.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Desired strong knowledge with Microsoft suite applications with majority in PowerPoint, SharePoint, and Teams Planner.

Desired Number of Participants: 1

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-032

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-032

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: J7, Readiness Division

Mission: Provide comprehensive readiness, exercise, assessment, and continuity program management to DISA Headquarters, Field Offices/Field Commands, and Cybersecurity Service Provider, to improve the Agency's readiness, resilience, and capability to provide the network and tools necessary to deliver capacity and capability to our warfighters.

Vision: To implement an effective assessment program to ensure the Combat Support Agency delivers a resilient warfighting network to meet today and tomorrow's threats.

Rotation Opportunity

Title: Cyber Exercise Planner

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Effects - Cyberspace Operator (322)
- Cyberspace Enablers - Cyber Instructional Curriculum Developer (711)
- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)

Location: Fort George G. Meade, Maryland (No. 009)

Work Schedule: Five-days on-site is the desired. Open to consider flexibility for remote work and/or telework based upon what is allowed by executive department policies.

Travel Requirements: Yes

Duration: 12 months

Description: Perform as a cyber exercise planner to develop, plan, and execute Agency-level exercises for the 18k-person military/civilian/contractor workforce. Participants would expect to be assigned to lead or support a major exercise as well as perform other duties that support Agency training and readiness.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: As a joint staff position that provides exercise planning for the overall Agency, participants can expect to gain the following: ability to turn strategic direction into operational directives to in turn execute tactical actions; opportunity to interact with senior leadership (General Officer/Senior Executive Service) on a reoccurring basis; and insight into how to increase readiness for a large organization through exercises and training.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-033

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-033

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: Cyber Security Service Provider

Mission: DISA CSSP delivers a suite of cybersecurity services on behalf of aligned Mission Partners designed to monitor for and protect against malicious actors, report cyber incidents, and share pivotal cyber situational awareness that supports Department of Defense (DoD) Information Network (DoDIN) defense and Mission Partner terrain.

Vision: J34-CSSP is responsible for improving overseas contingency operations (OCO) by synchronizing and validating agency campaign requirements. J34 leads, conducts, and shapes the risk management CIP program ensuring the availability of the DoDIN defense critical infrastructure. Additionally, J34 assists senior leadership across the DoW to prioritize investments throughout the DoW to ensure mission success.

Rotation Opportunity

Title: Mission Partner Liaison

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - IT Project Manager (802)
- Cyberspace Enablers - Program Manager (801)

Location: Chambersburg, Pennsylvania (Letterkenny Army Depot)

Work Schedule: Primarily Onsite – Willing to discuss alternatives

Travel Requirements: No

Duration: 12 months

Description: Provide a concise description of the expected opportunity duties, roles, or responsibilities. We recommend drafting the description as general as possible, while keeping in mind that opportunities are to be further tailored to the individual participant.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Customer support, leading projects from request to delivery of a FOC solution, excellent oral and written communications, project management, problem solving skills, creativity. IT certifications specifically CISM helpful.

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-034

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-034

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: DISA Global Field Command, Operations Division

Mission: DISA Global delivers and defends the Department of Defense Information Network (DoDIN) Area of Operations DISA (DAO DISA), enabling the warfighter and mission partners to conduct continuous global operations.

Vision: A trusted and empowered team of professionals who enable Department of Defense operations – worldwide, 24 hours a day, 7 days a week, 365 days a year.

Rotation Opportunity

Title: AI Machine Learning

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - AI/ML Specialist (623
- Data/AI - Data Scientist (423)

Location: Scott AFB, Illinois 62225 and/or Defense Supply Center Columbus, Ohio 43213 (No. 11)

Work Schedule: Rotation will be on site with situational telework available.

Travel Requirements: No

Duration: 12 months

Description: This rotation offers participants the chance to apply AI/ML to anomaly detection, threat identification, and performance management, gaining unique exposure to how intelligent technologies enhance DoDIN operations and cybersecurity defense at the enterprise scale.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Gain practical experience applying AI/ML concepts in a real-world DoD enterprise operations environment.
- Develop an understanding of how AI/ML can support NetOps and DCO missions at scale.
- Build skills in anomaly detection, predictive analysis, and model evaluation in mission-critical networks.
- Collaborate with operations, cybersecurity, and engineering teams to integrate AI/ML into daily workflows.
- Contribute to DISA Global's role as a leader in advancing enterprise-level automation and intelligent decision support.
- AI/ML literacy (understands concepts, not necessarily a data scientist).
- Operational awareness (knows how NetOps and DCO missions' function).
- Analytical skill (can interpret and apply outputs).
- Communication ability (can explain findings and integrate them into ops/engineering).
- Mission focus and adaptability (can apply new tools to solve real operational problems).

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other:

- Participants must have a baseline understanding of AI/ML concepts (e.g., supervised vs. unsupervised learning, anomaly detection techniques, performance metrics).
- This opportunity is designed for personnel seeking to bridge AI/ML research and real-world operations in support of DoD missions.
- Participants will not be required to code or build models from scratch but should be comfortable evaluating, applying, and interpreting AI/ML outputs in operational and engineering contexts.

Back to Top

Opportunity Number: DA-DoW-FRCWP-26-035

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DA-DoW-FRCWP-26-035

Host Organization

Name: U.S. Army - Department of the Army (DA)

Division: Network Command (NETCOM)

Mission: NETCOM is the Army's single information technology service provider for all network communications, we plan, engineer, install, integrate, protect, and operate Army Cyberspace, enabling Mission Command through all phases of Joint, Interagency, Intergovernmental, and Multinational operations.

Vision: NETCOM 2030 is the premier communications organization and information services provider to all DoDIN- Army customers worldwide, ensuring all commanders have decision advantage in support of mission command within the multi-domain environment.

Rotation Opportunity

Title: Analyst

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Cyber Defense Analyst (511)

- Cybersecurity - Cyber Defense Forensics Analyst (212)
- Cybersecurity - Cyber Defense Incident Responder (531)
- Cybersecurity - Vulnerability Assessment Analyst (541)

Location:

- Fort Huachuca, AZ
- Schofield Barracks, HI
- Cam Humphreys, ROK
- Wiesbaden, Germany

Work Schedule:

Travel Requirements: No

Duration: 3-12 months

Description: Global Cyber Center (Fort Huachuca AZ) or Regional Cyber Centers (Schofield Barracks -HI, Camp Humphreys Korea, or Wiesbaden Germany) . Initially created as a provisional organization in March 2023, the U.S. Army Global Cyber Center operates under the United States Army Network Enterprise Technology Command where it plans and conducts continuous operations and defense of networks, as directed, in support of cyberspace operations within or relating to the Army Department of Defense Information Network in order to ensure United States and Coalition forces freedom of action within cyberspace and deny our adversaries the same.

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Strong cyber defense and analysis skills.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Candidate's skills will be assessed against the position.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-036

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-036

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: DISA Global Field Command, Operations Division

Mission: DISA Global delivers and defends the Department of Defense Information Network (DoDIN) Area of Operations DISA (DAO DISA), enabling the warfighter and mission partners to conduct continuous global operations.

Vision: A trusted and empowered team of professionals who enable Department of Defense operations – worldwide, 24 hours a day, 7 days a week, 365 days a year.

Rotation Opportunity

Title: Cybersecurity Watch Officer

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Cyber Defense Analyst (511)
- Cybersecurity - Cyber Defense Incident Responder (531)

Location: Scott AFB, Illinois 62225, and/or Defense Supply Center Columbus, Ohio 43213 (No. 12)

Work Schedule: Rotation will be on site with situational telework available.

Travel Requirements: No

Duration: 12 months

Description: The Defense Information Systems Agency (DISA) Global Field Command (DGFC) provides continuous command and control of Department of Defense Information Network (DoDIN) operations and Defensive Cyberspace Operations (DCO) in support of Combatant Commands, Services, and mission partners. This rotation offers personnel an opportunity to serve within DG3's Current Operations, Boundary Defense, and CSSP Branches, gaining experience in real-time monitoring, incident response, and defensive cyberspace

operations. Additionally, the rotation will include integration into the Engineering Division to better understand DISN architecture, configurations, and sustainment.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Gain hands-on experience in DoDIN operations and defensive cyber missions within a 24/7 Active–Active construct the support DCDC equities.
- Develop familiarity with DISA's cyber defense tools, incident management systems, and reporting processes.
- Enhance skills in threat detection, incident handling, and operational reporting in direct support of mission partners and higher headquarters (DISA Joint Operations Center, DCDC).
- Build relationships with DISA Global's contractor workforce (GSMO), service liaisons, and HQ stakeholders.
- Contribute as the execution arm of DISA Global Field Command in managing and defending the DAO DISA.

- Cyber Defense Analyst (511)
    - Oversee the monitoring network and security tool telemetry for anomalies and suspicious activity.
    - Analyze event and incident data to identify potential threats or operational impacts.
    - Correlate information across DoDIN transport, boundary, and cybersecurity systems to enhance situational awareness.
    - Document findings and support development of Commander's Critical Information Reports (CCIRs), Director's Operational Incident Reports (DOIRs), and Director's Critical Information Requirements (DCIRs).

- Cyber Defense Incident Responder (531)
    - Assist in triaging and investigating suspected or confirmed cyber incidents.
    - Support containment, mitigation, and recovery actions directed by Cybersecurity Watch Officers.
    - Apply defensive countermeasures (e.g., indicators, signatures, firewall rules) under guidance.
    - Contribute to incident reports, After Action Reviews (AARs), and Requests for Information (RFIs).
    - Participate in technical exchange bridges and battle drills supporting real-world incidents or contingency operations.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: DA-DoW-FRCWP-26-037

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DA-DoW-FRCWP-26-037

Host Organization

Name: U.S. Army - Department of the Army (DA)

Division: Army Cyber Command Headquarters

Mission: U.S. Army Cyber Command conducts full-spectrum cyberspace operations, integrated with land, air, maritime, space and special operations, to ensure freedom of action in cyberspace for the U.S. and its allies, while denying the same to our adversaries.

Vision: U.S. Army Cyber Command (ARCYBER) is the supporting Army headquarters under United States Cyber Command.

We operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation with over 16,000 Soldiers, civilians, and contractors working 24/7 across the globe.

Rotation Opportunity

Title: ArCTIC – Research and Innovation Program Manager

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers – Program Manager (801)
- Cyberspace Enablers – IT Project Manager (802)
- IT – Research and Development (R&D) Specialist (661)

Location: Augusta, GA

Work Schedule: On-site, M-F, 0800-1600

Travel Requirements: No

Duration: 12 months

Description: Serve as a Research and Innovation Program Manager in the ARCYBER Technology and Innovation Center (ArCTIC). The ArCTIC Laboratory, reporting directly to the ARCYBER Commanding General and located at Fort Gordon, Georgia, is responsible for cyber-peculiar advanced research, prototype development, and pilot capabilities that satisfy ARCYBER operational requirements for time-sensitive operations. ArCTIC is committed to advancing Army modernization by delivering cutting-edge capabilities, fostering innovation, and strengthening partnerships. Through focused initiatives, ArCTIC enhances operational effectiveness, optimizes resources, and maintains the Army's competitive advantage in cyberspace and multi-domain operations (MDO). This position is an opportunity to serve as a Research and Innovation Program Manager within the ArCTIC. This detail provides an excellent opportunity to manage a variety of complex research projects focused on cyberspace, electronic warfare, AI, and future capabilities in direct support of the ARCYBER mission and its Warfighters.

- The selectee will function as an IT Project Manager and R&D Specialist for a portfolio of innovative, data-centric laboratory projects. They will engage in the planning, organizing, and execution of complex analytical studies and initiatives associated with developing future capabilities that involve cyber, AI, and electronic warfare initiatives.
- The work involves acting as a program manager and technical lead, guiding projects from the initial concept phase through prototype development and evaluation. The selectee must identify key technical challenges and opportunities, reflecting ArCTIC's data-centric mission in meetings with users, academic partners, and other project stakeholders.
- As a contributing Data Officer for these projects, the selectee will develop new ways to measure program accomplishments and the mission impact of emerging technologies. As such, the incumbent will coordinate efforts and advise ArCTIC leadership on project feasibility, resource requirements, and the potential for long-range system integration, ensuring research aligns with strategic goals.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of program management, R&D, and DAWIA principles, with a strong understanding of how data science, AI, cyberspace, and electronic warfare capabilities can be applied to the ARCYBER mission.

- Ability to manage the complete lifecycle of innovative technology projects, from the initial planning and organization of studies through to prototype development and evaluation.
- Ability to communicate and collaborate effectively with a diverse range of stakeholders, including operational users, academic partners, and senior leadership, to guide project development and ensure mission alignment.
- Ability to analyze the feasibility and resource requirements of complex technical projects and brief findings, status, and strategic recommendations to ArCTIC and ARCYBER leadership.
- Knowledge of emerging trends in cyber, AI, and electronic warfare, with an ability to identify innovative opportunities and translate them into concrete R&D initiatives to enable the success of the Warfighter.

Desired Number of Participants: 1

Security Clearance Requirement: No Clearance through TS/SCI with Polygraph.

Special Requirements/Other: PM-Practitioner (or above) and/or PMP certified preferred but not required.

Back to Top

Opportunity Number: DISA-DoW-FRCWP-26-038

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DISA-DoW-FRCWP-26-038

Host Organization

Name: Defense Information Systems Agency (DISA)

Division: Europe Field Command, EU33 Current Operations

Mission: DISA Europe provides, operates, maintains, and defends to assure DoDIN Enterprise Solutions and capabilities while executing unified command and control throughout the full spectrum of operations supporting USEUCOM, USAFRICOM, and other mission partners.

Vision: DISA Europe provides a secure, data-centric, coalition enterprise that enables access to critical information at the speed of decision for the warfighter and mission partners.

Rotation Opportunity

Title: DISN Netops Center Battle Captain

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cybersecurity - Cyber Defense Incident Responder (531)

Location: Patch Barracks, USAG Stuttgart, Germany (No. 13)

Work Schedule: On-site. Monday – Friday or shift work, as required.

Travel Requirements: No

Duration: Up to 6 months

Description: An opportunity for two (2) GS/GG-12/13 employees to perform the duties as a DNC Battle Captain and Incident Manager for the DISA Europe Field Command, Operations Division (EU3), Current Operations Branch (EU33).

Ideal Candidate

Knowledge, Skills, and Abilities Expected: Be part of the team supporting two major real-world operations by providing oversight, awareness, and reporting on incidents affecting the DISN to three combatant commands and DISA/DCDC leadership. Previous or current DNC Watch Floor experience desired but not required. Should be able to conduct briefings to leadership of both DISA Europe, DISA HQ, and CCMD J6 leaders.

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Applicants with previous or current Watch Floor experience as a Watch Officer or Battle Captain are highly encouraged to apply. Due to increased mission requirements in support of two active conflicts within theater, key qualifications include expert written and verbal communication skills, proficient knowledge of network operations, and strong decision-making skills.

Back to Top

Opportunity Number: DA-DoW-FRCWP-26-039

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DA-DoW-FRCWP-26-039

Host Organization

Name: U.S. Army - Department of the Army (DA)

Division: Army Cyber Headquarters

Mission: U.S. Army Cyber Command conducts full-spectrum cyberspace operations, integrated with land, air, maritime, space and special operations, to ensure freedom of action in cyberspace for the U.S. and its allies, while denying the same to our adversaries.

Vision: U.S. Army Cyber Command (ARCYBER) is the supporting Army headquarters under United States Cyber Command.

We operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation with over 16,000 Soldiers, civilians, and contractors working 24/7 across the globe.

Rotation Opportunity

Title: Data Management and Analytics Directorate – Integration and Data Division - Data Operation Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - Data Operations Specialist (624)

Location: Fort Gordon, Georgia

Work Schedule: Mon-Fri (8:00 am -5 pm), Onsite (Situational Telework)

Travel Requirements: No

Duration: 6-12 months

Description: An opportunity for multiple individuals to provide planning and analysis in support of work across ARCYBER as a Data Operation Specialist. Seeking (1) person for the role. This detail provides an excellent insight into discovering and performing a variety of complex

duties/projects, identifying guidance or courses of action to inform senior leadership on long-range strategic data objectives.

- The selectee must perform data operations of organizational importance, and reflect organizational positions on the ARCYBER Enterprise Data Architecture in meetings with users, contractors, industry, and mission partners.
- The work involves functioning as a Data Operations Specialist in their role in support of ARCYBER operations, plans and readiness management. The selectee will engage in planning, organizing, and completing broad and complex data operations studies and initiatives associated with the development and implementation of comprehensive, ARCYBER-wide capabilities.
- The work involves influencing Army DCO and DODIN operations to better utilize data as a strategic asset as well as day-to-day monitoring of ARCYBER's Data Catalog/inventory of data.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of ARCYBER's Data Centric Operations strategic initiatives
- Ability or experience to communicate and collaborate with representatives of the ARCYBER Enterprise, USCYBERCOM, DCDC, and other agencies.
- Ability to gather, formulate, and develop data operations requirements in response to ARCYBER directives, guidance and/or objectives.
- Ability to brief senior leadership on assessments, complex findings, and recommendations.
- Have knowledge about the data ecosystem powering Gabriel Nimbus
- Be familiar with the ARCYBER Data Catalog for all operational data types, tagging decisions, and characterizations

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret

Special Requirements/Other: Must possess appropriate clearance/access to work in the SCIF. Candidate's skills will be assessed against the position.

Back to Top

Opportunity Number: DA-DoW-FRCWP-26-040

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DA-DoW-FRCWP-26-040

Host Organization

Name: U.S. Army - Department of the Army (DA)

Division: Army Cyber Command (ARCYBER)

Mission: The Cyber Protection Brigade hunts advanced adversaries to enable decision dominance in multi-domain operations.

Vision: We are Cyberspace experts. We operate, maintain and defend strategic cyber infrastructure. We are uniquely trained. Leveraging exquisite intelligence and partnerships to drive cyberspace operations.

Rotation Opportunity

Title: Cyber Protection Brigade (CPB) - Data Operation Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - Data Operations Specialist (624)

Location: Fort Gordon, Georgia

Work Schedule: Mon-Fri (8:00 am -5 pm), Onsite (Situational Telework)

Travel Requirements: Up to 30% annually

Duration: 6-12 months

Description: An opportunity for multiple individuals to provide planning and analysis in support of work across CPB as a Data Operation Specialist. Seeking (1) person for the role. This detail provides an excellent insight into discovering and performing a variety of complex duties/projects, identifying guidance or courses of action to inform leadership on long-range Defensive Cyberspace Operations data objectives.

- The selectee must perform data operations of organizational importance and reflect organizational positions on the ARCYBER Enterprise Data Architecture in meetings with users, contractors, industry, and mission partners.
- The work involves functioning as a Data Operations Specialist in their role in support of CPB DCO operations, plans and readiness management. The selectee will engage in planning, organizing, and completing broad and complex data operations studies and initiatives associated with the development and implementation of comprehensive, BDE DCO capabilities.
- The work involves influencing Army DCO and DODIN operations to better utilize data as a strategic asset as well as day-to-day monitoring of CPB and ARCYBER's Data Catalog/inventory of data.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of ARCYBER and CPB's Data Centric Operations strategic initiatives
- Ability or experience to communicate and collaborate with representatives of the ARCYBER Enterprise, USCYBERCOM, DCDC, and other agencies.
- Ability to gather, formulate, and develop data operations requirements in response to ARCYBER and CPB directives, guidance and/or objectives.
- Ability to brief senior leadership on assessments, complex findings, and recommendations.
- Have knowledge about the data ecosystem powering Gabriel Nimbus
- Be familiar with the ARCYBER Data Catalog for all operational data types, tagging decisions, and characterizations

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Must possess appropriate clearance/access to work in the SCIF. Candidate's skills will be assessed against the position.

Back to Top

Opportunity Number: DA-DoW-FRCWP-26-041

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – DA-DoW-FRCWP-26-041

Host Organization

Name: U.S. Army - Department of the Army (DA)

Division: Army Cyber Command (ARCYBER)

Mission: The Cyber Protection Brigade hunts advanced adversaries to enable decision dominance in multi-domain operations.

Vision: We are Cyberspace experts. We operate, maintain and defend strategic cyber infrastructure. We are uniquely trained. Leveraging exquisite intelligence and partnerships to drive cyberspace operations.

Rotation Opportunity

Title: Cyber Protection Brigade (CPB) - Data Operation Specialist

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Data/AI - Data Operations Specialist (624)

Location: Fort Gordon, Georgia

Work Schedule: Mon-Fri (8:00 am -5 pm), Onsite (Situational Telework)

Travel Requirements: Up to 30% annually

Duration: 6-12 months

Description: An opportunity for multiple individuals to provide planning and analysis in support of work across CPB as a Data Operation Specialist. Seeking (1) person for the role. This detail provides an excellent insight into discovering and performing a variety of complex duties/projects, identifying guidance or courses of action to inform leadership on long-range Defensive Cyberspace Operations data objectives.

- The selectee must perform data operations of organizational importance and reflect organizational positions on the ARCYBER Enterprise Data Architecture in meetings with users, contractors, industry, and mission partners.
- The work involves functioning as a Data Operations Specialist in their role in support of CPB DCO operations, plans and readiness management. The selectee will engage in planning, organizing, and completing broad and complex data operations studies and initiatives associated with the development and implementation of comprehensive, BDE DCO capabilities.
- The work involves influencing Army DCO and DODIN operations to better utilize data as a strategic asset as well as day-to-day monitoring of CPB and ARCYBER's Data Catalog/inventory of data.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of ARCYBER and CPB's Data Centric Operations strategic initiatives
- Ability or experience to communicate and collaborate with representatives of the ARCYBER Enterprise, USCYBERCOM, DCDC, and other agencies.
- Ability to gather, formulate, and develop data operations requirements in response to ARCYBER and CPB directives, guidance and/or objectives.
- Ability to brief senior leadership on assessments, complex findings, and recommendations.
- Have knowledge about the data ecosystem powering Gabriel Nimbus
- Be familiar with the ARCYBER Data Catalog for all operational data types, tagging decisions, and characterizations

Desired Number of Participants: 2

Security Clearance Requirement: Top Secret

Special Requirements/Other: Must possess appropriate clearance/access to work in the SCIF. Candidate's skills will be assessed against the position.

Back to Top

Opportunity Number: USMC-DoW-FRCWP-26-042

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – USMC-DoW-FRCWP-26-042

Host Organization

Name: U.S. Marine Corps - Deputy Commandant for Information (DC I)

Division: Information Command, Control, Communications, and Computers (IC4)

Mission: IC4 supports the Deputy Commandant for Information (DCI) in their role supporting the Commandant of the Marine Corps as a member of the Joint Chiefs of Staff and represents the Service in Joint, Department of Defense, and Department of the Navy (DoN) C4 and Information Technology (IT) matters. In support of DCI, the division executes the functions of the DoN Deputy Chief Information Officer ((DDCIO) Marine Corps), the DoN Deputy Senior Information Security Officer (Marine Corps), and the Marine Corps Authorizing Official.

Vision: Enable the effective and efficient application, modernization, functional integration, acquisition, and management of all Marine Corps C4/IT resources that ensure Marines can communicate in any clime and place.

Rotation Opportunity

Title: Information Technology Specialist (Policy and Plans)

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)
- Cyberspace Enablers - IT Investment/Portfolio Manager (804)

Location: HQMC, Pentagon, DC

Work Schedule: Situational Telework

Travel Requirements: No

Duration: 12 months

Description: The major duties of this opportunity include evaluating, developing, and implementing high-level IT policies and guidelines that impact major technology programs and

projects. The role requires conducting in-depth research and analysis on complex IT issues, such as portfolio management, enterprise architecture and systems integration.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- KNOWLEDGE of advanced IT principles, concepts, and methods to develop strategic documents and define future state IT requirements.
- KNOWLEDGE of IT acquisition processes
- KNOWLEDGE of the design, limitations, and applications of advanced transmission systems, IT hardware, and software, with a focus on communications networks and cyberspace.
- KNOWLEDGE of current IT and cyberspace trends to influence technology insertion and strategic objectives.
- SKILL in the Service/DoD/Joint planning process to effectively represent USMC interests and influence high-level program objectives.
- SKILL in oral and written communication, with the ability to prepare and present persuasive briefings on complex and controversial issues to senior management and non-technical authorities.
- ABILITY to understand and shape strategic messages related to joint, interagency, and coalition IT/cyberspace issues.

Desired Number of Participants: 2

Security Clearance Requirement: Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: USMC-DoW-FRCWP-26-043

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – USMC-DoW-FRCWP-26-043

Host Organization

Name: U.S. Marine Corps - Deputy Commandant for Information (DC I)

Division: Information Command, Control, Communications, and Computers (IC4)

Mission: IC4 supports the Deputy Commandant for Information (DCI) in their role supporting the Commandant of the Marine Corps as a member of the Joint Chiefs of Staff and represents the Service in Joint, Department of Defense, and Department of the Navy (DoN) C4 and Information Technology (IT) matters. In support of DCI, the division executes the functions of the DoN Deputy Chief Information Officer ((DDCIO) Marine Corps), the DoN Deputy Senior Information Security Officer (Marine Corps), and the Marine Corps Authorizing Official.

Vision: Enable the effective and efficient application, modernization, functional integration, acquisition, and management of all Marine Corps C4/IT resources that ensure Marines can communicate in any clime and place.

Rotation Opportunity

Title: Enterprise Strategy Manager

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)
- Cyberspace Enablers - Program Manager (801)
- Cyberspace Enablers - IT Investment/Portfolio Manager (804)
- IT (Cyberspace) - Enterprise Architect (651)

Location: HQMC, Pentagon, DC

Work Schedule: Situational Telework available

Travel Requirements: No

Duration: 12 months

Description: Key responsibilities include drafting and staffing policy directives with Subject Matter Experts (SMEs), leading discussion groups to solicit input from the user community and resolving complex issues to ensure policies are practical and aligned with Enterprise objectives. Additionally, the manager participates in IT working groups to define enterprise-level acquisition and implementation strategies and engages in status reviews to ensure execution aligns with strategic plans and achieves projected efficiencies.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

Knowledge

- Advanced IT principles, concepts, methods, and standards.
- Interrelationships of multiple IT specialties
- New and emerging IT developments, applications, and their business application.
- IT security concepts, standards, and methods.
- Project management principles for planning, resource estimation, and monitoring.

Skills & Abilities

- Policy and Strategy: Develop, interpret, and govern the planning and delivery of IT services.
- Technical Guidance: Provide expert advice and recommendations on critical IT issues.
- Problem-Solving: Apply new developments to resolve complex problems.
- Systems Management: Design, develop, manage, and integrate IT systems to meet business requirements.
- Project Management: Manage projects, including developing plans, estimating resources, defining milestones, and reporting on accomplishments.
- Communication: Communicate complex technical requirements to non-technical personnel and present briefings to senior management.

Desired Number of Participants: 1

Security Clearance Requirement: Top Secret

Special Requirements/Other:

Back to Top

Opportunity Number: USMC-DoW-FRCWP-26-044

Anticipated Start Date: July 27, 2026

Apply Here: Cyber Rotation Programs Application – USMC-DoW-FRCWP-26-044

Host Organization

Name: U.S. Marine Corps - Deputy Commandant for Information (DC I)

Division: Information Workforce Division (IWD)

Mission: IWD leads the human capital strategy for the Marine Corps Information Enterprise, serving as the principal advisor to the Deputy Commandant for Information on all personnel matters. IWD directs the Corps' STEM and Cyber workforce programs and acts as the Chief Human Capital Officer for Marine Corps Intelligence, ensuring alignment with DoD and Navy directives.

Vision: To forge and sustain a world-class information and intelligence workforce, empowered with premier STEM and cyber expertise, to ensure the Marine Corps' decisive advantage in the information environment.

Rotation Opportunity

Title: Marine Corps Cyberspace Workforce Talent Management

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Workforce Developer and Manager (751)
- Cyberspace Enablers - Program Manager (801)

Location: HQMC, Pentagon, DC

Work Schedule: Telework available

Travel Requirements: May need to travel, will depend on budget

Duration: 12 months

Description: We are seeking a visionary to join our team and become a key architect of a people-centric culture. In this you will be building the future of Cyberspace Workforce Talent Management in the Marine Corps.

In this opportunity, you will champion our most valuable asset: our people. Your mission will be to design and implement innovative strategies for attracting top-tier talent, fostering their growth, and ensuring they have the tools and opportunities to build a fulfilling career with us. You'll be instrumental in shaping a workplace where every employee feels valued, engaged, and empowered to reach their full potential.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of Talent Management Principles
- Knowledge of Cyber Workforce Frameworks and Strategies
- Skill in Data Analysis
- Skill in Communication
- Skill in Project Management
- Skill in Coaching and Development
- Ability to Think Strategically
- Ability to Influence and Negotiate
- Ability to Solve Complex Problems
- Ability to Build Relationships

Traits:

- Empathy
- Adaptability
- Proactivity

Desired Number of Participants: 1

Security Clearance Requirement: Secret

Special Requirements/Other:

Back to Top

Opportunity Number: J6-DoW-FRCWP-26-045

Anticipated Start Date: October 1, 2026

Apply Here: Cyber Rotation Programs Application – J6-DoW-FRCWP-26-045

Host Organization

Name: Joint Staff J-6

Division: J6 - Command, Control, Communications & Computers (C4) / Cyber, Cyber & Information Systems Division (CISD)

Mission: The Joint Staff J-6 provides expertise in support of the Chairman's core responsibilities and in advancing C4/Cyber across all domains to enable a globally integrated Combined/Joint Force.

Vision: The lead Joint Staff advocate for the integration, modernization, and innovation of C4/Cyber capabilities for the Combined/Joint Force.

Rotation Opportunity

Title: Joint Staff J6 Cyber Rotational Position

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- Cyberspace Enablers - Cyber Policy and Strategy Planner (752)

Location: Pentagon

Work Schedule: Five days onsite

Travel Requirements: No

Duration: 12 months

Description: This position is assigned to The Joint Staff, J6 Directorate for Command, Control, Communications, and Computers / Cyber, Deputy Directorate-Command, Control, Communications, Computers, Cyber Employment and Modernization, Cyber & Information Systems Division (CISD).

The mission of the Joint Staff J6 is to provide expertise in support of the Chairman of the Joint Chiefs of Staff (CJCS) core responsibilities and in advancing C4/Cyber across all domains to enable a globally integrated Combined/Joint Force.

Cyber & Information Systems Division (CISD) is responsible for editing and authoring DoD instructions, plans, publications, and capabilities requirements related to defense cyber operations and cybersecurity. These documents are strategic in nature and directly impact CCMDs and the Joint Force.

- Engages in technical analysis and integration of information to advise the leadership of the Joint Chiefs of Staff of all things that support Defense Cyber Operations and cybersecurity issues, policies, and capabilities.
- Assists in defining, developing, and formulating recommendations for assigned areas on analytic approach, required policies and procedures.
- Conducts analysis involving integrated operations, exercise planning and cyber capabilities to collect, process, exploit, and disseminate accurate and timely information

that provides the battlespace awareness necessary for combatant commanders and other customers to successfully plan and conduct operations.

- Supports the development and maintenance of the cyber portfolio of the C4/Cyber FCB and for producing timely analyses related to issues in these functional areas.
- Prepares written statements, policy and correspondence for Chairman, Director JS and J6, Director, and other senior representatives on the Joint Staff and OSW on issue relating to C4/Cyber for defensive cyber operations.
- Prepares briefings for senior leaders on a variety of complex issues and to discuss issues in individual or group setting.
- Understands and influences all processes to deliver capabilities and Best Military Advice (BMA)to the Chairman, Director JS, J6 Director, and other senior representatives on the Joint Staff and OSW Staff on issue relating to C4/Cyber for defensive cyber operations.
- Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Engage in technical analysis and integration of information to advise the leadership of the Joint Chiefs of Staff of all things that support Defense Cyber Operations and cybersecurity issues, policies, and capabilities.
- Assist in defining, developing, and formulating recommendations for assigned areas on analytic approach, required policies and procedures.
- Analyze integrated operations, exercise planning and cyber capabilities to collect, process, exploit, and disseminate accurate and timely information that provides the battlespace awareness necessary for combatant commanders and other customers to successfully plan and conduct operations.
- Support the development and maintenance of the cyber portfolio of the C4/Cyber FCB and for producing timely analyses related to issues in these functional areas.
- Prepare written statements, policy and correspondence for Chairman, Director JS and J6, Director, and other senior representatives on the Joint Staff and OSW on issue relating to C4/Cyber for defensive cyber operations.
- Gain an understanding of all processes to deliver capabilities and Best Military Advice (BMA)to the Chairman, Director JS, J6 Director, and other senior representatives on the Joint Staff and OSW Staff on issue relating to C4/Cyber for defensive cyber operations.
- Gain knowledge and expertise in developing cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives

Desired Number of Participants: 1

Security Clearance Requirement: TS/SCI

Special Requirements/Other:

Back to Top

Opportunity Number: USMC-DoW-FRCWP-26-046

Anticipated Start Date: July 27, 2026

Apply Here: DoW Cyber Rotation Programs Application – USMC-DoW-FRCWP-26-046

Host Organization

Name: United States Marine Corps (USMC) – Deputy Commandant for Information (DCI)

Division: Information Maneuver Division (IMD)

Mission: IMD is directly responsible for developing and integrating strategy, policy, and initiatives that guide and enable resourcing, employment, and readiness assessments across Information functions and capabilities that maneuver in the information environment. IMD supports the USMC Information Enterprise by coordinating with key stakeholders across Marine Corps. IMD leverages relationships with Naval, other Service, joint, and interagency partners to ensure the Marine Corps has an unmatched capability for Information Activities.

Vision: IMD functions as a bridge connecting all the Information capability areas. IMD supports cyberspace operations, space operations, electromagnetic warfare/electromagnetic spectrum operations, Military Information Support Operations, Civil Affairs operations, military deception, exercise support, and 17XX OCCFLD management.

Rotation Opportunity

Title: Tactical Cyber Integration

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- 332 (Cyber Operational Planner)

Location: Camp Pendleton, CA; Camp Lejeune, NC; Pentagon, DC

Work Schedule: Situational Telework

Travel Requirements: None

Duration: 12 Months

Description: This opportunity will lead the development of the "Cyber-Tactical Employment Guide," which defines how Cybersecurity MOS Marines protect the Tactical Grid during deployed operations.

This position offers a unique "ground floor" opportunity for a civilian to shape the future of Marine Corps tactical cyber defense and support the transition to a more resilient, data-centric force.

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

- Knowledge of emerging technologies and their projected impact on cyber warfare and doctrine.
- Knowledge of joint and service-level doctrine development processes and the institutional levers for enacting systemic change.
- Ability to translate broad strategic guidance and future forecasts into actionable workforce modernization plans.
- Ability to conceptualize and implement innovative solutions to systemic workforce challenges.
- Skill in conducting long-range strategic planning to forecast future force structure, training, and equipment needs.
- Skill in performing comprehensive skill-gap analysis to compare current workforce capabilities against future mission requirements.
- Develop, write, and staff policy, doctrine, and strategic plans that redefine and modernize the cyber occupational field.

Desired Number of Participants: 3 (1 at each location)

Security Clearance Requirement: Top Secret

Special Requirements/Other: N/A

Back to Top

Opportunity Number: CAN-IN-CITEP-26-047

Anticipated Start Date: July 27, 2026

CCG

Apply Here: DoW Cyber Rotation Programs Application – CAN-IN-CITEP-26-047

Host Organization

Name: Canfield Consulting Group, LLC d/b/a Canfield CyberDefense Group (CCG)

Division: Division of Information Security Technology (DIT)

Mission: To deliver secure, innovative, and mission-driven cybersecurity and advanced technology solutions that protect critical infrastructure, strengthen digital resilience, and support both commercial and Government Agencies

Vision: To be a trusted leader in AI-powered cybersecurity and advanced Insider Threat defense technologies, advancing secure digital transformation and strengthening national and enterprise security.

Rotation Opportunity

Title: Cybersecurity Infrastructure & Systems Engineering

DoW Cyber Workforce Framework (DCWF) Work Role Code(s):

- 451 – System Administrator
- 441 – Network Operations Specialist
- 461 – Systems Security Analyst
- 621 – Software Developer
- 673 – Software Test & Evaluation Specialist
- 624 – Data Operations Specialist
- 622 - Secure Software Assessor
- 651 - Enterprise Architect

Location: 4110 Aspen Hill Rd, Rockville, Suite #300, MD 20853,

Work Schedule: This rotation opportunity will be conducted primarily on-site to support mission requirements and enable direct collaboration with operational teams.

Travel Requirements: No

Duration: 12 months

Description: Canfield CyberDefense Group (CCG) is seeking participants in the areas listed below who will perform hands-on operational duties supporting enterprise cybersecurity activities. Participants will engage in data analytics, threat monitoring, vulnerability assessments, system security analysis, secure configuration management, and AI-enabled system evaluation.

Participants will support incident response activities, network and database security operations, and technical troubleshooting within mission-focused environments. Duties will include applying cybersecurity best practices, supporting risk mitigation strategies, and contributing to the protection and secure operation of enterprise systems.

Participants will serve in roles such as:

- System Administrator – Supporting secure system configuration, user access management, and operational maintenance.
- Database Administrator – Managing database integrity, implementing security controls, and supporting performance monitoring.
- Network Analyst – Conducting network monitoring, traffic analysis, and anomaly identification.
- Technical Support Specialist – Providing operational and user-level technical support.
- Vulnerability Assessment Analyst – Identifying system vulnerabilities and recommending mitigation strategies.
- Secure Software Assessor – Reviewing software implementations for security compliance.
- Information Systems Security Developer – Supporting secure system design and implementation.
- Information Systems Security Manager – Assisting with governance, risk management, and security policy execution.
- Systems Security Analyst – Supporting security monitoring and defensive operations.
- Data Analyst – Performing data analysis to support operational insight and risk evaluation.
- AI/ML Specialist – Supporting AI model development, validation, and performance testing.
- AI Test & Evaluation Specialist – Testing AI-enabled systems for reliability and effectiveness.
- AI Risk & Ethics Specialist – Supporting AI risk analysis and ethical compliance considerations.

  .

Ideal Candidate

Knowledge, Skills, and Abilities Expected:

The ideal candidate will demonstrate technical proficiency in cybersecurity infrastructure, secure systems engineering, and automation. The following knowledge, skills, and abilities are expected:

Knowledge:

- Linux operating systems and Linux stack architecture
- Bash shell and PowerShell scripting environments
- System administration and system architecture principles
- Cisco networking technologies
- VMware virtualization environments
- Dell sensors and enterprise hardware infrastructure
- Juniper firewall configuration and security controls
- Programming languages: (Python, Java, JavaScript, Ruby)
- Web development technologies: (PHP, HTML, JavaScript)
- Configuration management tools: (Puppet and Ansible)
- Secure system configuration and cybersecurity best practices

Skills:

- Administering and securing Linux-based systems
- Developing and troubleshooting Bash and PowerShell scripts
- Configuring Cisco networking devices and Juniper firewalls
- Managing VMware virtualized environments
- Supporting Dell hardware and sensor-based infrastructure
- Writing and maintaining applications using Python, Java, JavaScript, and Ruby
- Supporting web-based applications using PHP, HTML, and JavaScript
- Implementing infrastructure automation using Puppet and Ansible
- Performing system security hardening and vulnerability remediation

Abilities Expected:

- Ability to design and maintain secure Linux-based system environments
- Ability to troubleshoot network, firewall, and virtualization issues
- Ability to automate system configuration and deployment processes
- Ability to analyze system logs and security events
- Ability to integrate development, infrastructure, and security practices

- Ability to work across engineering teams to support secure enterprise operations

Desired Number of Participants: 13

Security Clearance Requirement: Not Required

Special Requirements/Other:

- Must be a U.S. Citizen.
- Possess or be eligible to obtain and maintain an appropriate security clearance (Not a must but would be good to have).
- Must be able to work on-site in support of mission requirements (Hybrid, would be based on Leadership Approval)
- Must be able to handle sensitive or controlled information in accordance with federal security policies.
- Demonstrated interest in cybersecurity, data analytics, AI, or defensive cyber operations.
- Ability to work effectively in a team-oriented, mission-focused environment.
- Strong analytical and problem-solving skills.
- Effective written and verbal communication skills.
- Willingness to learn new tools, technologies, and security frameworks.
- Ability to follow established security procedures and compliance standards.

Opportunity Number: USN-DoW-FRCWP-26-048

Anticipated Start Date: July 27, 2026

Apply Here: **DoW Cyber Rotation Programs Application – USN-DoW-FRCWP-26-048**

Host Organization

Name: U.S. Navy

Division: PEO Digital

Mission: Provide the Marine Corps and Navy with a decisive information advantage through a modern, innovative, and secure digital experience – ***any data, any time, anywhere***.

Vision: Deliver a world-class digital experience ***at the speed of mission***.

Rotation Opportunity

Title: Multiple (Solution Train Management/Agile Release Trains; NEN Directorate; Enterprise IT Contracting aaS)

DoW Cyber Workforce Framework (DCWF) Work Role Code(s): Various

Location: WNY Bldg 196, Floor 3, Suite 301

Work Schedule: Onsite, ~0800-1630

Travel Requirements: TBD

Duration: 6 to 12 months

Description: As a rotational member within PEO Digital, you will be an immediate team member whether at the PEO Digital Express Solution Train level, within an Agile Release Train in support of a Product Manager, or as a Servant Leader within the Naval Enterprise Network Directorate in support of the Solution Train in delivering capability through contracting to the sailor and marine. If you are excited by relentless innovation towards rapidly exploring new ideas, scaling proven solutions and decisively retiring legacy systems, this is the PEO rotation for you!

Ideal Candidate

Knowledge, Skills, and Abilities Expected: [Not necessary to have all]

- Knowledge of Information Technology (IT) Business Systems acquisition laws, regulations and processes.
- Knowledge of Agile, Software Modernization and DevSecOps principles and processes.
- Skill in product/service management related to Enterprise Information Technology /Programs/ Systems/Defense Business Systems.
- Skill in risk management principles and processes, and the ability to terminate efforts or pivot if initial delivery assumptions were invalid or if there is a strategic opportunity.
- Skill in Continuous Process Improvement principles and methods.
- Skill in strategic thinking, planning, and executing enterprise IT service strategies.
- Skill in developing plans and strategies to develop and execute short- and long-range goals, objectives, and plans.
- Ability to exercise leadership, organize work and prioritize assignments in a high-pressure environment ensuring the achievement of milestones and incremental delivery of value to the end user.

Desired Number of Participants: 1-4

Security Clearance Requirement: Secret or above

Special Requirements/Other: A growth mindset