MINISTRY of DEFENSE ADVISORS (MoDA)
Position Description: KUWAIT – Senior Cyber Advisor

COCOM: CENTCOM
Location: Kuwait City, Kuwait
Title: Senior Cyber Advisor
Tour length: 18 to 30 months
Grade: GS-14/15
Clearance Level: Secret

Eligibility: Applicants must be DoD Civilians in GS 14/15 pay grades or Title 10 Faculty

Background

The Kuwaiti Ministry of Defense (KMOD) plans to establish a new Cyber Directorate. The KMOD has not yet defined the new organization's roles and missions nor has it settled on an organizational structure or staffing. KMOD leadership seeks assistance in developing a cyber strategy and cyber policies that will shape the new Cyber Directorate and to help the organization's leadership develop the organizational structure and workforce necessary to perform the Cyber Directorate's missions.

The Senior Cyber Advisor will support leadership at the KMOD, General Staff, the Kuwait Service branches, as well as the leadership of the Cyber Directorate. The primary expectation for the Senior Cyber Advisor will be to assist in the drafting and promulgation of cyber strategy and policy to bring about the necessary organizational, operational, and culture change necessary to improve cyber defense across defense institutions. Secondarily, the Senior Cyber Advisor will be expected to serve as a technical expert and resource for integrating information network operations, conducting defensive cyber operations-internal defense measures, and defensive cyber operations-response actions to include supply chain and the integration of business, office system, and control systems (platform information technology) to ensure Mission Partner cyber resilience.

A well-qualified applicant will demonstrate significant experience in applying the doctrine, organizational design, training, leadership development, material, personnel, facilities, and policy (DOTMILPF-P) construct in a cyber context.

Qualifications Summary

A successful Senior Cyber Advisor will develop strong cross-cultural relationships built on trust and technical competence with senior leaders across the defense institutions in order to help them promulgate clear guidance and bring about institutional, organizational, and cultural change. A good candidate will be comfortable assessing cyber capabilities and with the technical skills and certifications necessary to perform cyber functions and operations in any defense organization. A well-qualified candidate will have experience drafting cyber strategy and organizational-level cyber policy guidance. Interagency experience in drafting cyber strategy, establishing policy across departments/ministries, setting and clarifying organizational roles and responsibilities, and/or cyber incident response is a big plus. A strong candidate will have familiarity with cyber organizational development to include the design and development of a cyber workforce, budgeting and resource management for cyber capabilities, and cyber acquisition. Familiarity with all aspects of defense management process and decision-making will be of great value in advising leadership. Excellent written and oral communications skills are a must. Must be a self-starter with strong open-source cyber strategic research capabilities.

Specific Tasks

- Continually assess the strategic, operational, tactical, and technical cyber capabilities of Kuwait's defense institutions.
- Assist in the drafting of a defense cyber strategy.
- Assist in the establishment and promulgation of cyber-related policies that improve cyber security and cyber defense within defense institutions.

- Assist the senior leadership of Kuwait's defense institutions to implement the defense cyber strategy and bring about necessary reforms and changes.
- Assist in budgeting and securing resources necessary for cyber capabilities.
- Assist in cyber acquisition planning to ensure resources are prioritized for the most important defense cyber missions.
- Assist in developing cyber defense capabilities focused on protecting critical defense infrastructure, information systems, defense installations and facilities, communications networks, and tactical ground communications.
- Assist the defense institutions in refining understanding of cyber roles and missions including those required in support of other ministries or agencies.
- Support the development of an interagency framework to strengthen cyber defense capabilities across all sectors.
- Establishment of cyber operations doctrine, policies, procedures that enable the training, sustainment, and resourcing of a cyber workforce to accomplish defense objectives in cyberspace.
- Advise defense institutions and leadership on risk-informed decision-making in cyber modernization and the use of current technology, practice, and procedures (i.e., cloud services, zero trust, multi-factor authentication).
- Assist in the establishment of a cyber-aware culture within the Kuwait defense institutions.
- Advise, assist, and coordinate, as appropriate, with the U.S. Country Team (specifically the cyber advisor and the office of military cooperation), CENTCOM, Defense Security Cooperation Agency, Defense Technology Security Administration, and other U.S. government and allied stakeholders.
- Assist other security cooperation and information sharing efforts relating to cybersecurity capabilities.

Required Skills and Experience

- A bachelor's degree relevant to national security and cybersecurity, computer science, or information systems.
- Demonstrated experience applying cyber-related doctrine, organizational design, training, leadership development, material, personnel, facilities, and policy (DOTLMPF-P) framework in U.S. or international cyber organizations.
- Exceptional oral and written communication skills.
- The ability to provide advice and support to/with senior leaders to help them achieve mission and operational goals.
- Proven track record in developing, coaching, and mentoring people.
- Ability to apply innovative and creative solutions to solve problems in an environment with limited resources.
- Track record as a self-starter working successfully and independently or within a team at various organizational levels with executives, managers, and leaders from multiple U.S. government and Host Nation functional areas.
- Exceptional interpersonal skills with demonstrated ability to adapt to and thrive in different cultural environments.
- Working knowledge of current cyber threats and the U.S. government and private sector best practices both in use and in development to mitigate risk to data, networks, systems, and platforms.
- Familiarity with cyber training and education pipelines, career management, and the use of progressive certifications for a cyber workforce.
- Experience drafting cyber strategy and/or organization-wide cyber policy guidance.
- Experience in implementing cyber strategies and policies.

- Ability to model and reinforce democratic values and ideals for our partners at all times and without exception.

Desired Knowledge, Skills and Experience

- Master's Degree preferred in a field related to cybersecurity, computer science, or information systems.
- Master's degree in national security, foreign policy, or defense strategy.
- Demonstrated leadership experience or training in implementing programs that impact and change culture and improve individual and organizational performance.
- Excellent research skills with focus on using open source materials to develop institutional capacity.
- Detailed understanding of how cyber commercial threat information is integrated into cyber threat information developed by national and allied partners, to be able to create a unified active threat picture.
- Thorough understanding of information technology operations including wide area networking, data center, and cloud capabilities (private/hybrid/public). Ideally includes understanding of internet of things, mobility, and zero trust security solutions.
- Understanding of how the NIST security framework and risk management supports cyber operations.
- Understanding of advanced forensic, Security Information and Event Management (SIEM), and how related cyber tools are used at tactical, operational, and strategic levels of cyber warfare.
- Thorough understanding of how cyber operations are integrated into a hybrid campaign that integrates cyber, information operations, and the economic/ informational/ diplomatic/ military instruments of national power.
- Knowledge of U.S. cyber operation and cyber intelligence doctrine and how to develop national institutional capacity to develop national cyber doctrine.
- Experience in cyber budgeting and/or acquisition.
- Information Security Management, Certified Ethical Hacking, and related certifications.
- Experience with training and working internationally with partner governments or their militaries.
- Understanding of DoD security cooperation processes and programs.
- Functional Arabic language skills; spoken and written.

Additional Information

- The selected MoDA will do a Temporary Change of Station (TCS) move to Kuwait City and receive post differential and Cost of Living Allowance (COLA) while assigned to post. COLA is calculated based on the comparative cost-of-living at the foreign post versus the cost-of-living in Washington DC. COLA is not a direct calculation of base salary multiplied by the COLA percentage, but rather a percentage of spendable income as determined by the Department of State. For more information about COLA, go to: https://aoprals.state.gov/content.asp?content_id=245&menu_id=74
- This position is eligible to receive Relocation Incentive Pay in accordance with 5 U.S.C. § 5753 and DSCA policy.
- It is incumbent upon the applicant to understand the entitlements when considering applying for this position, and it is recommended that applicants seek guidance from their organization's payroll activity to better understand how the entitlements are calculated and their impact on the applicant's personal income.

HOW TO APPLY

Interested applicants should submit the following:
1. Cover Letter: Summarize how your skills and capabilities align with the requirements
2. Complete, narrative chronological resume (include civilian GS grade or military rank for each position)
3. Current SF-50: **please redact SSN and date of birth**
4. Three (3) Supervisor References: Required from current supervisor and supervisors from prior deployments (substitutions allowed)
5. Documentation of command/ component approval to deploy

Submit complete application package to the MoDA Program Office email address:
dsca.ncr.bpc.list.moda@mail.mil

Command Approval to deploy is required:
Air Force Employees: Must submit approved AF Expeditionary Civilian application to the AF Expeditionary Civilian team prior to MoDA consideration. The employee is required to obtain WG/CC or equivalent approval, when approved submit application and resume to the AFPC Expeditionary Civilian team at afpc.expeditionarycivilian@us.af.mil for final AF action.
The AFPC team will submit to MoDA for consideration. The application and other information are available at the AF Expeditionary Civilian site:
https://usaf.dps.mil/teams/12852/SitePages/Home.aspx

Department of the Army Employees: Must submit documented endorsement for deployment by their command leadership to the MoDA recruiting team, for coordination with Army AG1CP:
dsca.ncr.bpc.list.modaprograminfo@mail.mil

Navy and US Marine Corps Employees: Click on the following link to the MoDA Application and Command Support Form for DON Employees:
https://portal.secnav.navy.mil/orgs/MRA/DONHR/OCHRStennis/Expeditionary%20Civilian%20Workforce/Forms/AllItems.aspx
Submit completed MoDA Application and Command Support Form for DON Employees to the group email inbox: OCHRSTE_EC@navy.mil. Ensure “MoDA” appears in the subject line.

Other DoD Agency Employees: Provide approval memo staffed through your appropriate Deployment Coordinator or agency headquarters.
*If you do not know your agency’s deployment coordinator, contact the MoDA recruiting team:dsca.ncr.bpc.list.modaprograminfo@mail.mil