Staff Consultant – Zero Trust Functional Management Office (FMO)

Location: US/Remote / Customer Location: The Pentagon
Clearance Requirements: None (Prefer Secret or above)

Position Summary

GC2IT seeks a knowledgeable and driven Staff Consultant to support the Department of the Air Force (DAF) Zero Trust (ZT) Functional Management Office (FMO) under Headquarters Air Combat Command (HQ ACC/A6) and the Chief Technology Office (CTO). The Staff Consultant provides strategic, analytical, and operational consulting to advance the Air Force's enterprise-wide adoption of Zero Trust principles. This position will assist in shaping policy, developing roadmaps, coordinating portfolio activities, and ensuring measurable progress toward Zero Trust implementation objectives across the Air Force enterprise**.**

Primary Responsibilities

Zero Trust Policy and Governance

- Maintain awareness of evolving cybersecurity guidance, policies, laws, and regulations; integrate new requirements into existing enterprise ZT strategies and architectures.
- Draft, format, and revise policy, strategy, and governance documents supporting DAF Zero Trust objectives.
- Provide advice and recommendations for implementation options, program execution, and capability convergence across portfolios.

Strategic Planning and Integration

- Coordinate with DAF and DoD stakeholders to align ZT implementation with national, departmental, and enterprise directives.
- Establish and operate processes within the ZT FMO to coordinate, track, and drive activities supporting ZT roadmaps, milestones, and Implementation Plans (I-Plans).
- Ingest strategic roadmaps, generate capability-specific I-Plans, and track deliverables to ensure timely, measurable outcomes.
- Conduct assessments of existing ZT activities and systems; identify architecture deficiencies and recommend corrective actions aligned with the DAF ZT Roadmap.
- Collaborate with Enterprise Information Technology (EIT) Portfolio Managers and Program Element Managers (PEMs) to synchronize Zero Trust service delivery and programming across DAF organizations.

Collaboration and Stakeholder Engagement

- Coordinate with portfolio managers, program offices, and cross-functional teams for all systems maintained or used by the DAF.
- Advise and assist Government leads in researching, documenting, and validating ZT requirements for new and existing systems.
- Serve as liaison between ZT FMO and SAF/CN, ensuring consistent communication, reporting, and alignment across enterprise initiatives.
- Perform SAF Action Officer (AO) duties, including creation, management, and tracking of taskers and correspondence.

Training, Communication, and Change Management

- Collaborate with stakeholders to develop and deliver Zero Trust–focused cybersecurity awareness, role-based, and operational training and education programs.

- Design and deliver realistic cyber exercise scenarios to validate operational readiness and workforce understanding of ZT principles.
- Develop executive-level briefings, reports, and metrics for senior leadership, including submissions to Congress, the Office of the Secretary of Defense (OSD), and DoD oversight bodies.
- Provide communication and change management support to promote enterprise adoption, standardization, and alignment across DAF organizations.
- Support program management, business process improvement, and standardization activities associated with Zero Trust execution.

General
- Participate in meetings, progress reviews, and integrated product teams and working groups.
- Draft, edit, and review documentation, correspondence, and technical reports.
- Provide records management, scheduling, and meeting/conference support functions.
- Develop and present briefings and training materials.
- Liaise and coordinate effectively with personnel at all organizational levels.
- Monitor emerging requirements and recommend integration strategies.

Education and Minimum Requirements
- Bachelor's degree in Business, Information Technology, Cybersecurity, or a related STEM field.
- Demonstrated experience with Air Force or DoD enterprise infrastructure, governance, policies, and procedures.
- Strong understanding of DoD cybersecurity frameworks including RMF, NIST, and DISA STIGs.
- Excellent communication skills with the ability to brief senior leaders and produce high-quality, executive-ready documentation.
- Proficiency with Microsoft Office applications. SharePoint, Power BI, and data visualization and reporting tools a plus.

Preferred Qualifications
- Master's degree and/or advanced certifications (PMP, ITIL, Cloud, CISSP, or equivalent).
- Experience supporting Air Force Enterprise IT modernization, Zero Trust architecture development, or cloud migration initiatives.
- Familiarity with Agile methodologies and digital transformation practices in federal environments.
- Certified Zero Trust Strategist (ZTS) – Cloud Security Alliance (CSA), NIST ZT Architecture Training, Microsoft Certified: Cybersecurity Architect Expert, or MIT xPro Zero Trust Strategy certification.
- Artificial Intelligence or Machine Learning–related training or certification.

PHYSICAL DEMANDS: The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions. While performing the duties of this job the employee is regularly required to climb, bend, stretch, walk, sit use hands to handle or feel; frequently use fingers to type; talk and hear; occasionally stand, kneel, stoop, crouch, bend, twist or reach out; may require lifting or moving 10 lbs.; frequently required to reach with hands and arms. Vision requirements for this position include close vision, distance vision, color vision, peripheral vision, depth perception, and ability to adjust focus.

WORK ENVIRONMENT: Work environment will have moderate noise when working in an office environment.

ADDITIONAL INFORMATION:

Equal Opportunity Employer - The Company does not discriminate based upon race, religion, color, national origin, sex, sexual orientation, gender, gender identity, gender expression, transgender status, sexual stereotypes, age, status as a protected veteran, status as an individual with a disability, or other applicable legally protected characteristics.

All applicants must be able to perform the essential functions of the position, including corresponding core job requirements, with or without reasonable accommodation. Reasonable accommodation may be made to enable individuals with disabilities (and others in accordance with applicable law) to perform the essential functions of the job, consistent with applicable laws and Company policy.

Please email inquiries to: jobs@gc2it.com