Cyber Security Lead

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus LLC is seeking an experienced Cybersecurity Lead to plan, implement, upgrade, and monitor security measures for the protection of all common services and cloud environments in support of an Oracle eBusiness, OCI hosted common services program. In this role, you will ensure appropriate security controls are in place to safeguard digital files and vital electronic infrastructure hosted on the Cloud One Oracle Cloud Infrastructure (OCI) platform and will serve as the contractor's primary ISSO responsible for maintaining the program's Authorization to Operate (ATO), managing the DoD Risk Management Framework (RMF) lifecycle, and sustaining SOC 1 Type 2 audit readiness. You will respond to computer security breaches, vulnerabilities, and incidents affecting the environment and embed security practices throughout the DevSecOps pipeline. A CISSP certification or higher, and demonstrated RMF experience are required. An active Secret clearance is required to start.

What you'll do

- Plan, implement, upgrade, and continuously monitor security measures for the protection of all networks, systems, data, and cloud infrastructure operating within the Cloud One OCI authorization boundary
- Serve as the contractor ISSO, owning the DoD RMF package lifecycle including system categorization, control selection, implementation, assessment, authorization, and continuous monitoring for all information systems
- Ensure appropriate security controls are in place and operating effectively to safeguard digital files, financial management data, and vital electronic infrastructure across all environments, in compliance with NIST SP 800-53, DISA STIGs, and applicable Cloud One security requirements
- Lead and coordinate the ATO process with the Authorizing Official (AO), Security Control Assessor (SCA), and ISSM; maintain and update the System Security Plan (SSP), Plan of Action and Milestones (POA&M), and all associated RMF artifacts on a continuous basis

- Detect, respond to, and document cybersecurity incidents, breaches, and vulnerabilities affecting environments; coordinate with DISA, Cloud One, and the Government ISSM as required for incident reporting and remediation
- Support SOC 1 Type 2 audit compliance for Federal Financial Management systems migrating to OCI, providing control evidence, audit artifacts, and liaison support to external auditors
- Collaborate with the DevSecOps Lead to embed security scanning (SAST, DAST, container image scanning) and RMF control validation into CI/CD pipelines for continuous ATO compliance
- Maintain the enterprise security posture across all environments, conducting regular vulnerability assessments, reviewing ACAS/SCAP scan results, and tracking remediation to closure within approved timelines
- Monitor security controls and system configurations for compliance with applicable STIGs, CCIs, and Cloud One security policies; generate and track POA&M items to resolution
- Advise the Program Manager and Technical Lead on cybersecurity risk, control gaps, and security architecture decisions, including OCI-native security services (Cloud Guard, Security Zones, OCI Vault, Bastion)
- Support the development and maintenance of security-related deliverables including Security/RMF Artifacts, DR/COOP security design documentation, and recurring posture reports
- Ensure near real-time Production-to-DR/COOP data replication and failover configurations meet security and data protection requirements
- Coordinate foreign ownership, control, and influence (FOCI) considerations and organizational conflict of interest (COI) disclosures with program leadership as required
- Support cybersecurity awareness and training to program team members and support security-related onboarding for all incoming personnel

Required Qualifications

- US Citizen
- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or related technical field
- 5+ years of progressive information security experience in a DoD or Federal environment, including direct experience as an ISSO or equivalent role
- Active CISSP (Certified Information Systems Security Professional) or higher relevant certification required at time of hire
- Demonstrated, hands-on experience managing the DoD Risk Management Framework (RMF) lifecycle, including SSP development, control assessment, POA&M management, and ATO maintenance
- Experience implementing, upgrading, and monitoring security measures for the protection of computer networks and information systems, including ensuring appropriate controls are in place to safeguard digital files and electronic infrastructure

- Experience responding to computer security breaches, vulnerabilities, and incidents in a DoD or Federal environment
- Familiarity with NIST SP 800-53, DISA STIGs, SCAP/ACAS scanning tools, and cloud security controls applicable to FedRAMP/DoD cloud environments
- Active DoD Secret clearance required to start; must be maintainable for the duration of the program

Preferred Qualifications

- Active Top Secret (TS) security clearance; candidates holding an active TS clearance will be given strong preference as the program's operational scope and data sensitivity may require TS access
- Experience as an ISSO for systems operating within a DISA-managed or Cloud One environment, including familiarity with IL4/IL5 authorization requirements and Cloud One tenancy security controls
- Hands-on experience with OCI security services including Cloud Guard, Security Zones, OCI Vault, Network Security Groups (NSGs), and OCI Bastion
- Experience supporting SOC 1 Type 2 audits for Federal Financial Management systems, including evidence collection, auditor liaison, and FISCAM/FFMIA compliance familiarity
- Familiarity with Oracle eBusiness Suite (eBS), Oracle Fusion Middleware, or Oracle database security hardening and patching
- Experience with STIG implementation and automated compliance scanning for Oracle database and middleware products
- Additional DoD 8140/8570 IAM-level certifications (e.g., CISM, GSLC, CCISO) or IAT-level certifications (e.g., CASP+ CE, CISA) are a strong plus
- Familiarity with the DoD Enterprise Services Management Framework (DESMF) and service management security considerations
- Prior experience supporting AFLCMC, BES Directorate, or a DoD ERP program of record

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.