Position- Lead Security and Privacy Consultant- Direct Hire
Compensation- 140-160k
Location- Project is in Topeka, KS
Duration- 24mths (then will be assigned different project)
Company- National Consulting Firm

Our Client is National Outsourcing Firm and they are looking to hire permanently for the below position. If interested, please contact Mendy Hist mhist@mmcgrp.com, 972-215-5064 for additional details.

******Applicants for employment in the U.S. must possess work authorization which does not require now or in the future* sponsorship by the employer for a visa.**

The Security and Privacy (KSP) Lead will be key member of the project team. This position will be long-term (24-month) and full-time. The position will report directly to the PMO. The Lead will be responsible for ensuring that meets all federal and state security standards and industry best practices.

The project has been provisionally assessed a security category (SC) of: (confidentiality, HIGH), (integrity, HIGH), (availability, HIGH). The solution is a mission-critical enterprise public-service delivery system that will be used by hundreds of businesses and hundreds of thousands of Kansas citizens and a key component to the delivery of healthcare in Kansas. The solution will utilize role-based access controls, with numerous security levels. The solution must securely interface with federal, state and insurance carrier systems.

The Lead will direct the contractors by providing input into development of deliverables. The Lead will be responsible for approving all security and privacy related deliverables.

The Lead will provide oversight for all aspects of security throughout the lifecycle of the project, i.e.

- **Requirements Analysis and Design** – Ensure that all security-related requirements are properly reviewed and accepted into the requirements management matrix; this will include derived requirements. Ensure that design documents and specifications adhere to all applicable federal and state security standards. Determine where industry "best practices" are and are not being followed by the Contractor. Assist the Contractor in defining security related design deliverables. Review and approve these deliverables.

- **Construction and Unit Testing** – Ensure that each solution component meets all security requirements defined during the design phase. Emphasis of this position is in

application security including authentication, authorization, role (groups, privileges), credential mapping, encryption and certification and keys.

- **Integration, System and User Acceptance Testing (UAT) –** Develop security-related testing plans including test scripts. Ensure that all security and identity management functionality and interfaces are thoroughly tested end-to-end to ensure there are no unacceptable vulnerabilities in the solution. Ensure UAT includes sufficient security and privacy test scenarios.

- **Training –** Review training material to ensure it adequately addresses user security and privacy topics.

- **Vulnerability Assessment and Penetration Testing –** Oversee the 3rd party contractor conducting the vulnerability assessment and penetration test in accordance with KITO requirements.

- **Risk Assessment and Security Plan** – Oversee the development of the risk assessment and security plan in accordance with KITO requirements and NIST document – "Risk Management Guide for Information Technology Systems," Publication 800-30.

- **Deployment** – Establish policies and procedures for managing and authorizing changes to KEES security profiles and assigning profiles to users.

There are eight major security and privacy controls and capabilities in the solution. The KSP Lead will oversee these controls across each phase of the project lifecycle.

- **System and Data Classification** – During the requirements analysis phase (ELC Design) all system data for will be classified. The capture, storage and transmission of this data will be determined by HIPAA requirements & IRS data safeguard requirements governing the reception and use of Federal Tax Information (FTI). For developing controls required for IRS data, the project is reaching out to the Kansas Department of Revenue to research IRC 6103 and IRS Publication 1075 for managing FTI.

- **Security Controls** – After classification data security requirements framework will be established using a risk-based approach. The State of Kansas embraces the NIST family classification of Security Controls and these will be incorporated in the design phase (from NIST SP800-53). These controls are closely aligned with the seventeen minimum security requirements for federal information and information systems as directed in FIPS 200.

- **Identity, Credential, and Access Management (ICAM)** – Oracle's COTS Identify Management solution was selected for identity proofing, authorization and authentication. (Helpful but not necessary.)

- **Secure Infrastructure and Cloud Computing** – The project will have a multi-zone architecture to ensure the solution has the capability to be used by additional states; this architecture extends to the security handler.

- **Data Encryption** – This control will address: 1) protection of confidentiality when sensitive data is in transit including email, 2) off-site back-up media as well as data residing on removable storage media or devices will be encrypted. The solution will use FIPS Pub 140-2 encryption algorithms.

- **Audit Trails** – Full audit trail capabilities have been demonstrated in the proposed KEES systems and will be implemented. These capabilities in totality will meet the requirements for HIPAA, PII and PHI data.

- **Compliance Oversight** – Each business partner will appoint an individual to manage security and privacy data; governing agreements will be required of each business partner; a preliminary security review will be conducted and a final review prior to deployment

- **Privacy** – the project will incorporate the principles in the Harmonized Security and Privacy Framework

Required Knowledge and Skills

- Knowledge of all aspects of application security in a SOA environment.
- Knowledge of the NIST family classification of Security Controls.
- Ability to make decisions at the project team level and properly escalate those decisions that cannot be resolved on a timely basis.
- Possesses good analytical skills.
- Demonstrates good presentation, oral and written communication skills.
- Working knowledge of the State's IT security policies and standards.
- Exhibits effective team and leadership skills.
- Knowledge of IT security controls for large healthcare systems.
- Willingness to acquire new knowledge and learn new skills.

The Lead will be required to obtain and maintain a Kansas Bureau of Investigation Level 2 Security Clearance.