Job Description

Classification: Information Technology Manager II

Position Title: Chief Information Security Officer

Position Number: 801-130-1406-005

Division/Branch: Information Technology Division

Location: Sacramento County

Job Description Summary

Under administrative direction of the Chief Information Officer, the Information Technology Manager II (ITM II), Chief Information Security Officer (CISO), oversees the Information Security Office. Develops and maintains information security policies for Covered California that incorporate applicable federal, state, local, and industry legal, statutory, and regulatory requirements. Ensures that personally identifiable information is protected with operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability, and to prevent unauthorized or inappropriate access, use, or disclosure. Ensures ongoing monitoring, assessments, and other methods are in place and updated to report and mitigate non-adherence, and oversees staff who serve as the primary liaison with federal, state, and internal auditors for audits of information security controls. This position serves under the domain of Information Security Engineering. Duties may include access to information systems containing protected enrollee information, including federal tax information, protected health information, and personally identifying information.

Job Description

35%(E)
Program Leadership and Management: Oversees the Information Security Office. Directs the Information Security Office's planning processes to establish an inclusive and comprehensive information security program. Establishes annual and long-range security and compliance goals, defines security strategies, metrics, reporting mechanisms and program services, and creates maturity and risk models and a road map for continual program improvements. Stays abreast of information security issues and regulatory changes affecting Health Benefit Exchanges, federal and state entities, and healthcare providers. Provides information security leadership for Covered California to create a strong bridge between business customers and partner organizations through education. Builds respect for the contributions of all and bring groups together to share information and resources to create better decisions, policies and practices. Mentors the Information Security Office team and implements professional development plans for all members of the team. Participates as a senior member of the Information Technology Division management team, including participation in the development and management of overall division organization, budget, strategic planning and training. Advises Executive Leadership on security trends, threats, and best practices. Establishes processes and programs to increase security awareness throughout the Department and with key business partners. Acts as primary liaison for Covered California for internal investigations requiring technology support. Develops plans to meet goals, leveraging staff skills, and solving problems; builds collaborative relationships and fosters an inclusive environment for consensus-building and decision-making; coaches, guides, trains, instructs, and develops team members; empowers staff through a sense of shared ownership and decision-making; creates an open and transparent environment for the exchange of information; fosters a team environment through the support and recognition of team members; promotes customer service and accountability; and motivates loyalty to the Department’s mission and commitment to drive continuous improvement for better results. Assigns work and priorities, monitors progress, adjusts priorities, redistributes workload, and secures extensions as needed to meet

established deadlines. Selects and hires staff and identifies training needs. Provides supervision, support, and guidance to staff consistent with policies and ensures uniform interpretation and implementation of laws, rules, regulations, policies, and procedures.

25%(E)
Policy Development: Provides Covered California and the California Healthcare Enrollment and Eligibility Retention System (CalHEERS) Project security program oversight and policy management. Develops and maintains information security policies for Covered California that incorporate applicable federal, state, local, and industry legal, statutory, and regulatory requirements. Develops and maintains information security requirements for external contracts and inter-agency agreements. Establishes and maintains required information security awareness training for the Department and external entities as appropriate. Establishes and maintains a Security Incident Response Plan for Covered California. Ensures external contractors have appropriate security incident response plans in place and identifies Covered California roles and responsibilities within those response plans. Establishes and implements ongoing security and privacy policies and standards consistent with 45 CFR §155.260 to ensure that personally identifiable information is protected with operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. Provides oversight and mentorship to the Information Security Officer (ISO) to ensure all of the above policies and procedures are also appropriately implemented and managed within CalHEERS

20%(E)
Compliance and Audit: Assesses, evaluates, and makes recommendations to executive and senior management regarding the adequacy of the security controls for the Department's information and technology assets including internal systems and assets maintained by external contractors. Works with internal audit, federal and state audit entities, and outside consultants with required security assessments and audits. Oversees and tracks all information technology and security related audit information including scope of audits, work plans, and any resulting Plan of Action and Milestones (POAM's). Maintains working relationships with audit entities. Provides guidance, evaluations, and advocacy on audit responses. Works with department leadership and relevant responsible compliance department leadership to build a cohesive security and compliance programs for the department to effectively address POAM's. Reviews and disseminates security related intelligence. Protects the use of Federal Tax Information (FTI) within Covered California including the safeguarding of FTI based on the Internal Revenue Code (IRC) 6103 and the Internal Revenue Service Publication 1075. Ensures that implementation of technology assets in the cloud are secure and comply with all security policies including securing approvals from the Centers for Medicare and Medicaid Services (CMS) and/or the Internal Revenue Service. Develops a road map to improve oversight and compliance with security policy for all external contracts and inter-agency agreements.

10% (E)
Risk Management and Incident Response: Manages security incidents and acts as primary control point during significant information security incidents. Convenes a Security Incident Response Team (SIRT) as needed or requested in addressing and investigating security incidences that arise. Provides leadership and mentorship to the ISO to ensure the appropriate management and security incidents for CalHEERS. Develops technical security standards and works collaboratively throughout the division and other business areas to ensure the implementation and monitoring of a suite of security services and tools to address and mitigate security risk. Provides direction, leadership, and guidance in assessing and evaluating information security risks and monitors compliance with security standards and appropriate policies. Examines impacts of new technologies on the department's overall information security framework. Establishes processes and reviews implementation of new technologies to ensure security compliance. Provides rotating after-hours and weekend support remotely or on-site as required to support department operations.

5%(M)

Information Security Architect: Serves as a member of the Enterprise Architecture team, contributes to enterprise architecture review, recommendations, planning and execution to ensure that technology solutions adhere to information security standards and industry best practices. Identifies security design flaws and proactively makes recommendations for improving designs security practices - balancing the business impacts with the potential risks. Recommends security practices which aligns with contemporary software development practices and strikes a balance between absolute, theoretically secure products and products which are demonstrably secure. Provides guidance and reviews changes to the methods for external connectivity to include authentication, encryption, application protocols, and intrusion detection. Works with security operations to develop initial proof of concept implementations of security solutions. Performs research, recommends solutions, and creates proposals based on latest industry trends, and industry standards to meet business requirements. Engages, defines and project manages third party software security audits and assessments. Collaborates with both internal and external users to improve proactive security position in workforce qualifications, system and technical architecture, and business processes.

5%(M)
Travels statewide to attend meetings and training, and also between other Covered California locations.

Scope and Impact
a. *Responsibility for Decisions and Consequences of Error:*
b. *Administrative Responsibility:*
c. *Supervision Exercised:*
d. *Frequent Internal Personal Contacts:*
e. *Frequent External Personal Contacts:*

Scope and Impact
a. Consequences of Error: This position serves in an upper management role in setting or influencing organizational information technology policy, formulating long-range information technology programs and objectives, and reviewing implementation and conformance of information technology programs with organizational policies, objectives, and law compliance. This position receives broad administrative and policy direction and requires little or no direct supervision. The CISO is responsible for working on extremely confidential and critical information security issues. The consequence of error is very high and enterprise-wide, as errors could expose consumer data (in the case of externally facing data) or cause inaccurate personnel actions to be taken (in the case of internal investigations).
b. Administrative Responsibility: The CISO manages the Information Security Office with a direct operating budget varying between $1 and $1.5 million. The CISO has responsibility for overseeing the information security efforts of both the entire Covered California information technology area as well as the CalHEERS project, with a combined total operating budgets of approximately $175 million (before cost allocation with other programs). The CISO is also responsible for including security compliance requirements in all external Covered California contracts.
c. Supervision Exercised: Information Technology Manager I, Information Technology Specialist II, Information Technology Specialist I
d. Internal Personal Contacts: Executive Director, Chief Deputy Executive Directors, Chief Information Officer, Chief Technology Officer, Divisional Directors, Deputy Directors, other managers and supervisors as needed, information technology staff, and other Covered California staff.
e. External Personal Contacts: State Chief information Security Officer, Federal Oversight entities, Federal and State Audit Managers, current and prospective vendors, CalHEERS State Management team, CalHEERS System Integrator Management and security team

Physical and Environmental Demands
WORK ENVIRONMENT

Work in a climate-controlled, open office environment, under artificial lighting; exposure to computer screens and other basic office equipment; work in a high-pressure fast-paced environment, under time critical deadlines; work strenuous and long hours; must be flexible to work days/nights, weekends and select holidays as needed; during peak enrollment periods, may be required to work overtime; appropriate dress for the office environment.

ESSENTIAL PHYSICAL CHARACTERISTICS

The physical characteristics described here represent those that must be met by an employee to successfully perform the essential functions of this classification. Reasonable accommodations may be made to enable an individual with a qualified disability to perform the essential functions of the job, on a case-by-case basis. Ability to attend work as scheduled and on a regular basis and be available to work outside the normal workday when required. Continuous: Upward and downward flexion of the neck. Frequent: sitting for long periods of time (up to 70%); repetitive use of hands, forearms, and fingers to operate computers, mouse, and dual computer monitors, printers, and copiers (up to 70%); long periods of time at desk using a keyboard, manual dexterity and sustained periods of mental activity are need; using headsets to talk with internal and external customers for extended periods (up to 60%); Frequent: walking, standing, bending and twisting of neck, bending and twisting of waist, squatting, simple grasping, reaching above and below shoulder level, and lifting and carrying of files, and binders. Note: Some of the above requirements may be accommodated for otherwise qualified individuals requiring and requesting such accommodations.

Working Conditions and Requirements

a. Schedule: Core business hours are Monday - Friday, 8:00am - 5:00pm, 8 hours per day, 40 hours per week. The incumbent may be required to work outside of standard business hours to support 24/7 service requests.

b. Travel: Travels statewide to attend meetings and training, and also between other Covered California locations up to 5% of the time.

c. Other: Incumbent is required to carry a department issued cellular telephone.