|  |  |  |  |
| --- | --- | --- | --- |
| Job Title: | Security Analyst | Job ID: | 64390 |
| Department/Group: | CO HCPF | Position Type: | Contract |
| Duration : | 07/07/2025 - 09/30/2025 | Date Posted: | 06/10/2025 |
| Expenses Allowed : | No | Posting Expires: | 06/16/2025 |
| **Location :** | Remote  **Address**  1570 Grant St Denver, Colorado  Candidate Must Be Local | **Quantity Requested :** | 1 |
| **Additional Location Details (City, State):** | Prefer Colorado candidates but not required | Send Resumes to : | resumes@taurusbiz.com |
| **Level/Salary Range :** | $70/hr on C2C |  |  |
| **Schedule:** | | | |
| **Days**  Monday Yes Tuesday Yes Wednesday Yes Thursday Yes Friday Yes Saturday No Sunday No  **Hours/Day**  8  **Time Zone**  MST  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Shifts Start Time End Time Description Active**    Shift 1 8:00 AM 5:00 PM Yes  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    **Description**  **SEE ATTACHED SOW FOR FULL POSITION DESCRIPTION**  **CBMS/PEAK Compliance Program Manager Contractor**  **Summary of the purpose of this position.**  This position is responsible for audits and compliance review in the development, enhancement and  maintenance of the Program Eligibility Application Kit (PEAK) and the Colorado Benefits Management System (CBMS), and any additional CBMS subsystems.  **This includes the following:**  Oversees the coordination of annual audits and serves as primary liaison to the audit teams during their  review of PEAK, CBMS and its subsystems compliance with documented processes. Coordinates the  collection of audit items/documents. Coordinates meetings and provides information as needed for  audit requests.  Performs Quality Assurance monitoring on documentation and other assigned items  **CBMS/PEAK Compliance Program Manager Contractor**  **Summary of the purpose of this position.**  This position is responsible for audits and compliance review in the development, enhancement  and maintenance of the Program Eligibility Application Kit (PEAK) and the Colorado Benefits  Management System (CBMS), and any additional CBMS subsystems. This includes the following:  ● Oversees the coordination of annual audits and serves as primary liaison to the audit  teams during their review of PEAK, CBMS and its subsystems compliance with  documented processes. Coordinates the collection of audit items/documents.  Coordinates meetings and provides information as needed for audit requests.  ● Performs Quality Assurance monitoring on documentation and other assigned items.  **Duties**  1. **SOC 1 Type 2 Audit Coordination** -  Brief Duty Description:  ● Coordinate with the CDHS CBMS SOC audit team and HCPF staff to provide HCPF  responses to requests from service auditors as necessary.  ● Serves as the primary lead Point of Contact for audits on PEAK, CBMS, OIT and its subsystems.  ● Serves as lead point of contract for Independent Verification and Validations  (IV&V) teams  ● Serves as lead point of contract for State of Colorado System and Organization  Controls (SOC) auditors and the Office of State Auditor (OSA)  ● Serves as point of contract for Social Security Administration (SSA) Audits  ● Collaboration with the program area leads, vendor representatives, IV&V  members, management, and others to provide support to the auditors.  ● Assist with the coordination of the collection and sharing of documentation, and  coordinate team members with the audit team.  ● Coordinates all audit findings and responses to ensure items are addressed and  resolved.  Specific examples of regular, ongoing decisions made by this position related to this duty.  ● MARSe 2 audit - coordinate resolution of controls with HCPF. This would include  determining who on the CBMS team would be assigned the Control. This position  would also manage updates and statuses of work being done on each control.  ● MEET (CMS) - coordinate resolution of controls with HCPF. This would include  reviewing controls and determining who on the CBMS team would be assigned  the Control. This position would also manage updates and statuses of work being  done on each control. ● Annual SOC 2 Type 2 audit - work with SOC auditors when to initiate audit and  then coordinate resolution of controls with OIT and vendor.  ● ADA compliance within CBMS, PEAK, mobile apps and subsystems (Atlassian  Suite, Google, etc).  In performing this duty, provide examples of typical problems or challenges encountered  by this position, and the guidance used to resolve the problem.  ● In the course of coordinating an audit, challenges with collection of support may  be encountered. Following the processes established and escalating to  management would be the steps to resolve the problem.  2. **Other Duties as Assigned** -  ● Identity & access management - identify user roles, security groups that should  exist, active directory cleanup assistance/coordination with appropriate teams  ● Understanding of PEAK/CBMS security architecture - network, cloud, data, etc.  ● Risk assessments  ● Vulnerability management  ● PEAK/CBMS specific compliance/security policies  ● Understanding of security configs.  ● Validation of security testing in CI/CD pipelines for deployments  ● Coordination with incident management and DR  **Compliance Tasks**  This section outlines the current CBMS compliance tasks and provides background information  about the requirements related to the tasks.  **Federal Data Services Hub (FDSH) Authority to Connect (ATC) Background**  The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing many  provisions of the Patient Protection and Affordable Care Act of 2010 (ACA). Accordingly, CMS  developed, assembled, and implemented a document suite of guidance, requirements, and  templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in  accordance with the Agency’s Information Security and Privacy programs. MARS-E provides  guidance on the protection of security and privacy in the ACA program environment; addresses  the mandates of the ACA, including regulations 45 CFR §§155.260 and 155.280; and applies to  all ACA Administering Entities (AE). Medicaid agencies such as HCPF are AEs under the ACA.  CMS has updated MARS-E periodically since its first publication in 2012 to ensure continued  compliance with the regulatory environment. Version 2.0 in November 2015 was the most  recent major update. In developing MARS-E v. 2.0, CMS relied on the CMS Acceptable Risk  Safeguards (ARS) v. 2.0, as the basis for the security and privacy control requirements. The  CMS ARS is based on National Institute of Standards and Technology (NIST) Special  Publication (SP) 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems  and Organizations. MARS-E v. 2.0 of the MARS-E Document Suite consisted of four volumes:  ● Volume I: Harmonized Security and Privacy Framework● Volume II: Minimum Acceptable Risk Standards for Exchanges  ● Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls  for Exchanges  ● Volume IV: ACA Administering Entity System Security Plan  MARS-E Version 2.2 is an interim release that reflects the updates to security and privacy  policies and standards guidance at the national, Department of Health and Human Services  (HHS), and CMS levels since 2015. The next major release, Acceptable Risk Controls for ACA  Medicaid-Partner Entities (ARC-AMPE), will incorporate CMS’s interpretation, tailoring, and  implementation guidance for NIST 800-53 Rev 5.2.  The ATC must be renewed every three years, when significant changes have occurred to the  control environment, or as directed by CMS.  **Tasks related to the FDSH ATC**  ● Participate in CMS meetings  o CO MED / CMS Security Discussion meetings (first Thursday of each month) –  This is a meeting between the CMS security team and HCPF.  o ACA State Administering (AE) Office Hours meeting (third Thursday of each  month) - This webinar will provide States with information on current specific  system topics via a slide deck, live demonstrations, and a question-and-answer  session.  ● ATC Readiness Review (ARR) – The ATC Readiness Review Process (ARR) for the  ACA Information Systems provides the overall process of ensuring that all the artifacts  submitted as part of the ATC package are finalized, and that all necessary requirements  are met. It highlights the required documents, the timeline for submission, and the roles  of the stakeholders in accordance with the MARS-E Security and Privacy controls  mandated by CMS. ARR meetings are held quarterly and begin one year prior to the  expiration of the ATC. Meeting attendees should include technical SMEs along with  business operations SMEs and leadership.  ● Plan of Action & Milestones (POAM) and Vulnerability Scans – The POAM and  vulnerability scans are required to be submitted to CMS on a quarterly basis (end of  January, end of April, end of July, and end of October).  **Social Security Administration (SSA) Security Assessment Background**  ● SSA conducts a security assessment on CBMS every three years. The security controls  that are assessed are very similar to the CMS security requirements so the most recent  Independent Third-Party Security/Privacy Assessment can be leveraged for most of the  assessment.  ● A POAM is created for any exceptions that are noted during the assessment and is  submitted to SSA quarterly or as directed by SSA  ● Requires coordination among CBMS technical, business operations, business  leadership, and other SMEs**Service and Organization Controls (SOC) Audit**  SOC 1 - Report on Controls at a Service Organization Relevant to User Entities’ Internal Control  Over Financial Reporting (ICFR)  ● Prepared in accordance with AICPA’s AT-C section 320, Reporting on an Examination of  Controls at a Service Organization Relevant to User Entities’ Internal Control Over  Financial Reporting  ● Specifically intended to meet the needs of user entities (state agencies) and the  individuals that audit the user entities’ financial statements (user auditors), in evaluating  the effect of the controls at the service organization on the user entities’ financial  statements  ● The Office of the State Auditor (OSA) is a user auditor to the state agencies  **Tasks related to the SOC 1 Type 2 audits (link to CDHS SOC process document)**  ● Review control objectives and complementary user entity controls (CUECs)  o At least annually  o HCPF needs to review the CUECs prior to the audit start to assess impacts to  SOC reports for other systems/vendors  ● Coordinate pre-audit activities with service auditors as necessary  o Identification of audit scope  o Identification of required meetings  o Receipt of audit request list and distribution to appropriate SMEs  ● Coordinate audit activities with service auditor and internal staff as necessary  o Review draft report  o Prepare management comments to noted exceptions  ● Review final report and provide summary information to leadership as necessary  o Management responses to findings should be assessed for appropriateness  o If necessary, a formal remediation plan may be requested  ● Release final report to OSC and OSA  o SOC reports must be delivered to OSC within 10 business days of receipt  ● Respond to questions from OSA, OSC, CMS, etc.  o Request extension, as necessary  o Coordinate responses among SMEs  o Attain appropriate leadership approval of the response prior to providing a  response to OSA**Current**  **Compliance and Audits List**   |  |  |  | | --- | --- | --- | | **Audit Name** | **Audit Type** | **When** | | SOC 1 Type 2 - Report on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting (ICFR) | Statement on Standards for  Attestation Engagements No. 16.  Type 2 SOC 1 effectively replaced SSAE 16 as the authoritative guidance for reporting on service organizations as of June 2018. The name SSAE 16 effectively replaced SAS 70 as of June 2011.  GE - Specifically intended to  meet the needs of user entities  (the Department) and the individuals that audit the user entities’ financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities’ financial statements | Annually - The goal is to have the final audit report  delivered by September or October. The Office of the  State Auditor (OSA) requires this report for the Single Statewide Audit. | | Minimum Acceptable Risk  Standards for Exchanges (MARS-E) Independent Third-Party Security Assessment | The assessments should include determining the strength of  CBMS’ technology that might allow a threat to enter the  infrastructure, evaluating the seriousness of that current threat posture; reviewing components for the ability to access restricted areas; checking that the network is appropriately  segmented to protect the data, reviewing for known exploits;  reviewing IT security  policies/procedures for compliance; and making recommendations, amongst  other items. | Annually - The authority to connect (ATC) to the Federal Data Services Hub (FDSH) must be renewed every three years. In years 1 and 2 of the ATC cycle,  the final security assessment report (SAR) must be completed prior to the Department's ATC anniversary date of August 18. In year 3 when the ATC must  renewed, the SAR must be completed at least 90 days prior to the ATC anniversary date  (May 18). | | System Security Plan (SSP) - part of ATC (Ability to Connect) security package; includes Privacy Impact Assessment, Interconnection Security Agreement, Annual Attestation, and other policies and procedures. | GE - This isn't an assessment or audit. However, this is a key  document that is reviewed by the assessment team as part of  the independent third-party assessment. | This should be reviewed/updated at least annually Prior to the  independent third-party assessment. In year 3 of the ATC cycle, this document must be  submitted to CMS as part of the ATC renewal security package. | | Social Security Administration (SSA) Security Assessment | GE- Similar to the independent third-party security assessment  required to be completed annually in accordance with MARS-E requirement.  The independent third-party security assessment report (SAR) can be leveraged as evidence for much of the SSA security assessment. | Every 3 years. SSA determines the specific timing of the assessment. | | Office of State Auditor (OSA) | Ongoing activities to be  determined |  | | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Reviewed By:** | Lisa G | **Date:** | 06/10/2025 |
| **Approved By:** | Ram S | **Date:** | 06/10/2025 |
| **Last Updated By:** | Lisa G | **Date/Time:** | 06/10/2025 |