|  |  |  |  |
| --- | --- | --- | --- |
| Job Title: | GA DHS - Application  Manager | **Region :** | State of Georgia |
| Req Class : | ITPROGMGR : IT Program Manager 1 | **Job Code/ Req#**: | 765322 |
| Engagement Type: | Contract | **Agency Interview Type:**: | Web Cam Interview Only |
| Location: | Remote  **Worksite Address:**  47 Trinity Ave SW, Atlanta, GA 30334 | **Start Date:** | 07/07/2025 |
| **Req. Status:** | Open | **End Date:** | 06/30/2026 |
| **Expenses Allowed:** | No | **No new Submittals after:** | 06/13/2025 |
| **No.of Openings :** | 1 | **Max Submittals by vendor per Openings :** | 2 |
| **Hours/Units Per Day :** | 8 | **Days Per Week :** | 5 |
| **Level/Salary Range :** | $68.09/hr on C2C | **Send Resumes to :** | resumes@taurusbiz.com |
| **Requisition Description** | | | |
| **Short Description:** The **Application Manager** will play a pivotal role in overseeing multiple application projects, ensuring seamless coordination between cross-functional teams and work streams.  **Complete Description:**  **Application Manager**  This individual will be responsible for managing project execution, monitoring team performance, ensuring optimal resource allocation, and overseeing vendor relationships. The Application Manager will also ensure that cross-work stream interactions are efficiently managed and that all deliverables align with business objectives, timelines, and quality standards. **A strong understanding of**  **technology security practices and familiarity with security policies and compliance requirements within state agencies are essential to this role.**  **Key Responsibilities:**  **Team Coordination & Cross-Work Stream Interaction:**  -Facilitate coordination between cross-functional teams and work streams to ensure effective communication, knowledge sharing, and alignment across departments.  -Drive collaboration between different teams, ensuring that each work stream is on track, with clear ownership and timelines.  -Act as the main point of contact between work streams, ensuring that dependencies between teams are identified and managed proactively.  **Project Oversight & Progress Monitoring:**  -Develop comprehensive project plans that outline clear goals, milestones,  deadlines, and responsibilities across multiple work streams.  -Track the progress of all work streams within a project, ensuring that individual  streams align with overall project objectives and timelines.  -Address any delays or issues that arise, ensuring smooth project progression and  that any interdependencies are handled efficiently.  **Resource Allocation & Bandwidth Management:**  -Monitor team capacity and bandwidth across work streams to ensure that resources are optimally allocated and that no team or individual is overburdened.  -Reallocate resources as needed to maintain a balanced workload and ensure highpriority tasks are completed on time.  -Ensure alignment of resources across multiple work streams to avoid conflicts and optimize productivity.  **Performance Tracking & Evaluation:**  -Continuously monitor and evaluate the performance of teams and work streams,  using data to assess productivity and identify areas for improvement.  -Provide regular feedback to team members and work stream leaders, identifying  opportunities for process improvements or resource adjustments.  -Report on the status of project deliverables and team performance to senior  leadership, offering insights and actionable recommendations.  **Task Progression & Outcome Evaluation:**  -Ensure the timely completion of tasks across work streams, making adjustments as  needed to accommodate shifts in priorities or resources.  -Evaluate the outcomes of completed projects, identifying key successes and areas  for future improvement.  **Risk, Security & Issue Management:**  -Proactively identify and address potential risks, including **cybersecurity vulnerabilities** or compliance issues, that may affect the progress or quality of work across different work streams.  -Develop risk **mitigation plans** and implement corrective actions promptly to keep projects on course.  -Ensure that all project risks, including those related to **security policies and data protection**, are communicated to stakeholders in a timely manner.  -Maintain familiarity with **state agency security regulations** and ensure that applications and systems comply with applicable **state and federal security policies** and standards.  **Security Collaboration & Guidance:**  -Work closely with enterprise security teams to review and validate security architecture for applications across cloud, on-premises, and hybrid environments.  -Provide ongoing security guidance to application development and DevOps teams, ensuring adherence to security best practices throughout the software development lifecycle (SDLC).  -Collaborate on the implementation of secure CI/CD pipelines, integrating security checks such as static/dynamic code analysis, secrets scanning, and artifact integrity verification.  -Guide teams on proper configuration and use of cloud security services (e.g., IAM, encryption, network security controls) in platforms such as AWS, Azure, or Google Cloud.  -Assist in developing and enforcing infrastructure security standards, including secure provisioning, patch management, and hardening of resources across environments.  -Participate in threat modeling and security risk assessments to proactively identify and mitigate vulnerabilities in application design and deployment strategies  **Vendor Management & Collaboration:**  -Oversee relationships with external vendors, ensuring they deliver products and  services on time and within agreed-upon terms.  -Collaborate with vendors to resolve any project-related issues and ensure that their  deliverables meet organizational and security standards.  -Ensure that vendor engagements include appropriate **security clauses**, and that  vendors adhere to **state-mandated cybersecurity practices**.  **Continuous Improvement & Process Optimization:**  -Identify opportunities to streamline workflows across work streams, improve communication, and increase efficiency.  -Implement best practices and process improvements to optimize project execution, resource allocation, and team collaboration.  -Continuously integrate **security best practices** into the application life cycle and project management methodologies.  **Qualifications:**  -10+years’ experience in application management, project oversight, and crossfunctional team coordination.  -Strong leadership and organizational skills with a demonstrated ability to manage and oversee multiple teams and work streams simultaneously.  -Proven experience collaborating with security architects and engineering teams to ensure secure application design and deployment.  -Strong understanding of cloud security principles, including identity management, encryption, and network segmentation.  -Experience with secure CI/CD practices and infrastructure-as-code security controls (e.g., Terraform, Ansible, GitOps).  -Familiarity with security tools and platforms, container security, vulnerability management, and SIEM systems.  -Demonstrated experience **with cybersecurity principles, secure application development, and** compliance with **state agency IT security policies**.  -Familiarity with regulatory frameworks such as **NIST, HIPAA, CJIS, or other relevant government security standards**.  -Experience in vendor management, including negotiation, performance tracking, and contract management.  -Expertise in project management tools and methodologies, with the ability to track performance and optimize resources effectively.  -Excellent communication skills with the ability to drive cross-functional collaboration and manage complex relationships.  - Strong problem-solving skills and the ability to manage risks and resolve issues in a timely manner.  **Required/Desired Skills**   |  |  |  |  | | --- | --- | --- | --- | | **Skill** | **Required /Desired** | **Amount** | **of Experience** | | Application management, project  oversight, and cross-functional team coordination. | Required | 10 | Years | | Strong leadership and organizational skills with a demonstrated ability to manage  and oversee multiple teams and work streams simultaneously | Required |  |  | | Proven experience collaborating with security architects and engineering teams to ensure secure application design and  deployment | Required |  |  | | Strong understanding of cloud security principles, including identity management, encryption, and network segmentation | Required |  |  | | Experience with secure CI/CD practices and infrastructure-ascode security controls (e.g., Terraform, Ansible, GitOps) | Required | 5 | Years | | Familiarity with security tools and  platforms, container security, vulnerability management, and SIEM systems | Highly desired |  |  | | Demonstrated experience with  Cyber security principles, secure application development, and compliance with state agency IT security policies. | Required | 5 | Years | | Familiarity with regulatory frameworks such as NIST, HIPAA, CJIS, or other relevant  government security standards | Highly desired |  |  | | Experience in vendor management, including negotiation, performance tracking, and contract management. | Required | 5 | Years | | Expertise in project management tools and methodologies, with the ability to track performance and optimize resources effectively | Required |  |  | | Excellent communication skills with the ability to drive crossfunctional  collaboration and manage complex relationships. | Required |  |  | | Strong problem-solving skills and the ability to manage risks and resolve issues in a timely manner. | Required |  |  |  |  |  | | --- | --- | |  | **Description** | | **Question 1** | Absences greater than two weeks MUST be approved by CAI management in advance and contact information must be provided to CAI so that the resource can be reached during his or her absence. The Client has the right to dismiss the resource if he or she does not return to work by the agreed upon date. Do you accept this requirement? | | **Question 2** | What is your candidate's email address? | | **Question 3** | This assignment is contingent upon customer renewal and availability of adequate funding. Do you agree to this requirement? | | **Question 4** | If selected for engagement, your candidate will be expected to start no later than 2 weeks (10 business days) after the client's selection date? Do you agree to this requirement? | | **Question 5** | Remote Work Permitted: Due to COVID-19, the client has agreed to allow the selected candidate to work remotely for the time being. However, the selected candidate must be available to report onsite as directed by the client. Do you accept this requirement? | | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |