Title:	DHCF DCAS - Lead Security Engineer	**Region:**	District of Columbia
Req ID:	724734		

Details

Requisition Details

Req. Class:	ST2BSAV1 : 4-Master	**Region:**	District of Columbia
Title:	DHCF DCAS - Lead Security Engineer		
Req. Status:	Open		
No. of Openings:	1	**No. Filled:**	0
Start Date:	01/29/2024	**End Date:**	09/30/2024
No New Submittals After:	01/18/2024		
Max Submittals by Vendor per Opening:	2		
CAI Contract Manager:	Todd Grimmett		
Worksite Address:	Remote		
Agency Interview Type:	Webcam Only		
Existing Incumbent Resource?:	No		
Contract:	STaR2		
Work Arrangement:	Remote		

Rate Information

Rate Structure used:	Straight Time - STaR2
Hours/Units per day:	8
Days per week:	5
Engagement Type:	Contract
Short Description:	The contractor is responsible for the organization's security program including but not limited to daily operations of the IT security program.

Complete Description:

The Security Lead will support the District of Columbia Access System (DCAS) under the Technical Program manager to identify security vulnerabilities, design, and implement security solutions, monitor security systems, and respond to security incidents impacting DHCF on-premises and cloud hosted resources. The contractor shall provide subject matter expertise in the design, development and implementation of security best practices which includes, but is not limited to, network security, application security, access control, and security policy development.

Responsibilities:

- Conduct security assessments and audits to identify vulnerabilities and provide recommendations for remediation of DHCF assets.
- Design, implement, and manage security infrastructure and tools, including firewalls, intrusion detection systems, vulnerability management systems, antivirus systems.
- Collaborate with IT teams to ensure security best practices are integrated into IT projects and operations for divisions providing services internally and externally.
- Develop and maintain security policies, procedures, and standards.
- Monitor security systems and respond to security incidents in a timely manner.
- Provide security awareness training to employees and stakeholders.
- Stay up to date with the latest security trends, threats, and technologies.
- Should have experience with Center for Medicaid Services (CMS), Internal Revenue Services (IRS) and Social Security Administration (SSA) Audits and Remediation.

Qualifications:

- Minimum of 15 years of experience working in the field of cybersecurity.
- Knowledge of federal and industry-specific regulations and compliance requirements related to cybersecurity (e.g., FISMA, HIPAA, GDPR).
- Experience in preparing for and participating in security audits and assessments.
- Expertise in network security, including firewalls, intrusion detection/prevention systems, and VPNs.
- Proven experience with security assessment tools and methodologies.
- Proficiency in security technologies such as SIEM (Security Information and Event Management) systems and endpoint protection solutions
- Experience with security monitoring tools, log analysis, and incident response procedures in Azure environments.
- Strong leadership skills with the ability to motivate and manage a team effectively.
- Excellent communication and interpersonal skills to work collaboratively with diverse teams and stakeholders.
- Demonstrated ability to develop and implement security policies, procedures, and standards.
- Experience in incident response, including conducting investigations and managing security incidents.
- Strong understanding of cloud security principles and best practices.
- Strong knowledge of network security, encryption, authentication methods, and security protocols.
- Excellent problem-solving skills and attention to detail.
- Strong communication skills and ability to work collaboratively with cross-functional teams.

Deliverables:
- Comprehensive cybersecurity strategy document outlining short-term and long-term goals.
- Updated security policies and procedures manual.
- Regular compliance reports and documentation of security measures taken.
- Security assessment reports detailing identified vulnerabilities and recommended remediation strategies.
- Documentation of implemented security measures and configurations.
- Incident reports for security incidents, including analysis, containment, eradication, recovery, and lessons learned.
- Create a detailed implementation plan outlining the steps and timeline for deploying security solutions, configuring firewalls, intrusion detection systems, and

other security tools.
• Integrate and configure security tools, such as SIEM (Security Information and Event Management) systems, intrusion detection systems, and vulnerability scanners, for continuous monitoring and threat detection.
• Develop a comprehensive incident response plan outlining procedures for identifying, containing, eradicating, recovering from, and documenting security incidents. Conduct tabletop exercises to validate the plan.
• Configure network security devices, including firewalls, routers, and switches, to enforce access controls, segmentation, and threat detection.
• Complete Remediation of all findings from audit reports and communicate with the federal agencies that conduct audit.

CONTRACT JOB DESCRIPTION
Responsibilities:
1. Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements.
2. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications.
3. Provides consultation on complex projects and is considered to be the top-level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.

Minimum Education/Certification Requirements :
Bachelor’s degree in IT or related field or equivalent experience; or a current Project Management Professional (PMP) Certification

Client Information

Work Location:	DHCF - 955 L'Enfant Plaza SW, Suite 3500, Washington DC 20024	**Cost Center:**	DHCF - Department of Health Care Finance
		Project:	DCAS

Required/Desired Skills

Required /Desired

Skill	Required /Desired	Amount	of Experience
16+ yrs. MS Office/PowerPoint experience	Required		
Bachelor’s degree in IT or related field or equivalent experience	Required		
Knowledge and exp in state and federal information security laws, including but not limited to HIPAA, including NIST, PCI and all other regulations	Required	8	Years
Proven expertise in presenting executive level reports on project security and compliance	Required	8	Years
Healthcare Privacy and Security (CHPS) certification and/or other healthcare industry related security credentials	Highly desired		
Proven track record in the successful completion of an SDLC	Required	10	Years

from a security workstream standpoint			
Expertise translating security protocols and requirements to stakeholders and/or technical project managers	Required	8	Years
Knowledge of project management tools - JIRA, SharePoint, Sciforma, Salesforce, MS Project (preferably)	Required	8	Years
Proven documentation expertise for the purpose of security policy development, audit finding responses, security risks/gap analysis reports etc.	Required	8	Years
Proven experience functioning as the prim POC for IT security audits	Required	8	Years
Knowledge of HIPAA, state and federal guidelines on security, transactions and security	Required	8	Years
Experience working in IT Security for the Health and Human Services sector	Required	10	Years
Expience managing a team of IT professionals specializing in IT Security	Required	10	Years
CISSP Certification (preferred)	Highly desired		
Excellent communication and leadership skills	Required	10	Years
Expert knowledge of the MS Office Suite	Required	10	Years
Knowledge and/or understanding of Curam - V6 or higher (desired)	Highly desired		
ITIL Certification (desired)	Highly desired		
Proven knowledge and expertise with health care relevant legislation and standards for the protection of health information and patient security	Required	7	Years
Professional Experience that Meets the requirements for a Master Level Business Systems Analyst	Required	16	Years

Questions

	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	Please list candidate's email address.
Question 3	Candidates submitted above the NTE vendor rate will not be considered. Do you accept this requirement?
Question 4	There are no reimbursable expenses. Do you accept this requirement?
Question 5	This position requires that, if selected for the role, candidate must provide proof of vaccination against COVID-19. Individuals may request an exemption which, if granted, would instead require weekly COVID-19 testing as well as mask wearing anytime they are onsite. Do you accept this requirement and affirm you will share this requirement with your candidate(s)?

Compliance

	Group Name	Linked	Global
	Onboarding Items		No
	Additional Onboarding Items		No

Reference

Requisition Comments

User Name	Org. Short Name	Date/Time	Comment	Sys. ID
	District of Columbia	01/11/2024 08:55 PM	The candidate rejected the offer so we are reopening for additional candidates.	18262923
	District of Columbia	11/21/2023 06:00 PM	We will not be increasing the number of submission openings.	18204480
		11/21/2023 05:58 PM	Good Afternoon -- Please can we have the lot increased so we can submit more candidates.	18204474