Title:	OCTO- Cyber Security Entprs Arch-Master	**Region:**	District of Columbia
Req ID:	530604		

Details

Requisition Details

Req. Class:	EARCV1 : 4-Master	**Region:**	District of Columbia
Title:	OCTO- Cyber Security Entprs Arch-Master		
Req. Status:	Open		
No. of Openings:	1	**No. Filled:**	0
Start Date:	04/11/2018		
No New Submittals After:	03/16/2018		
Max Submittals by Vendor per Opening:	2		

Worksite Address:	200 I Street NE, Washington,
Agency Interview Type:	Either Webcam or In Person
Advanced Technical Screening Required?:	No
Existing Incumbent Resource?:	Yes

Requisition Description

Engagement Type: Contract

Short Description: Secures enterprise information by determining security requirements; planning, implementing, and testing security systems; preparing security standards, policies, and procedures; mentoring team members.

Complete Description:

ENTERPRISE SECURITY ARCHITECT IS RESPONSIBLE FOR DEVELOPING BLUEPRINT FOR ENTERPRISE SECURITY ARCHITECTURE. DEFINES, PLANS, AND APPLIES ARCHITECTURAL ELEMENTS IN THE ANALYSIS, PLANNING, DESIGN, IMPLEMENTATION, DOCUMENTATION, ASSESSMENT, AND MANAGEMENT OF THE ENTERPRISE SECURITY ARCHITECTURE THAT IS ALIGNED WITH IT STRATEGY AND AGENCY MISSION, GOALS, STRUCTURE, AND PROCESSES. DEVELOPS SECURITY DESIGN REQUIREMENTS THROUGH SOUND DESIGN METHODOLOGY, ADEQUATE SECURITY CONTROL APPLICATION, AND EFFECTIVE CONFIGURATION PRACTICES. This role ensures secure architectural solutions are incorporated into every aspect of the enterprise architecture supporting an organization’s key business processes and organizational mission. The Cyber Security Architect will function as an interface between Program and Business Manager and the OCTO Information System Security Engineering team to develop and implement counter-measures to contain, control and recover from dynamic cybersecurity events. USES KNOWLEDGE ABOUT CURRENT THREATS TO IDENTIFY FLAWS AND WEAKNESSES IN THE COMPOSITION OF SYSTEM DESIGNS AND DEFENSES FOR THE MISSION AND MISSION CRITICAL DATA. SPECIFIES SOLUTIONS AND VERIFIES SOLUTIONS THAT HAVE BEEN IMPLEMENTED. RAPIDLY ADJUSTS DESIGNS BASED ON NEW DEFENSE, THREAT, AND ATTACK INFORMATION. SPECIFIC TASKS WORK INVOLVES THE ANALYSIS, PLANNING, DESIGN, IMPLEMENTATION, DOCUMENTATION, ASSESSMENT, AND MANAGEMENT OF THE ENTERPRISE STRUCTURAL FRAMEWORK TO ALIGN IT STRATEGY, PLANS, AND SYSTEMS WITH THE MISSION, GOALS, STRUCTURE, AND PROCESSES OF THE ORGANIZATION. DEVELOP ENTERPRISE SECURITY ARCHITECTURE FOR THE DISTRICT WORK CLOSELY WITH CROSS-FUNCTIONAL TEAMS AND PROVIDE FINAL REVIEW OF ALL DESIGNS UNDERSTAND CURRENT AS WELL AS EMERGING SECURITY THREATS. IDENTIFY SECURITY ARCHITECTURE CAPABILITIES AND DESIGN SECURITY ARCHITECTURE PATTERNS TO MITIGATE THREATS DOCUMENT AND ADDRESS ORGANIZATION'S INFORMATION SECURITY, INFORMATION ASSURANCE (IA) ARCHITECTURE, AND SYSTEMS SECURITY ENGINEERING REQUIREMENTS THROUGHOUT THE ACQUISITION LIFECYCLE; ENSURE ALL DEFINITION AND ARCHITECTURE ACTIVITIES (E.G., SYSTEM LIFECYCLE SUPPORT PLANS, CONCEPT OF OPERATIONS, OPERATIONAL PROCEDURES AND MAINTENANCE TRAINING MATERIALS) ARE PROPERLY DOCUMENTED AND UPDATED AS NECESSARY; DEVELOP AND MAINTAIN SECURITY STANDARDS INCLUDING, BUT NOT LIMITED TO, NETWORK INFRASTRUCTURE, WIRELESS AND MOBILE INFRASTRUCTURE, OPERATING SYSTEMS, DATABASES, APPLICATIONS, AND EMERGING TECHNOLOGIES ASSESS EMERGING TECHNOLOGIES AGAINST SECURITY ARCHITECTURE TO DETERMINE WHERE THEY FILL GAPS, OVERLAP WITH EXISTING SOLUTIONS OR EXTEND CAPABILITIES SERVE AS INFORMATION SECURITY SUBJECT MATTER EXPERT; PROVIDE ADVISORY AND CONSULTING SERVICES AS NEEDED REVIEW EXISTING AND PROPOSED ARCHITECTURES, IDENTIFY SECURITY DESIGN GAPS, AND RECOMMEND CHANGES OR ENHANCEMENTS PARTICIPATE IN SOLUTION ARCHITECTURE DESIGN; LEAD SECURITY EFFORTS ASSISTING WITH THE INTEGRATION AND INITIAL IMPLEMENTATION OF SOLUTIONS PERFORM SECURITY REVIEWS, IDENTIFY GAPS IN SECURITY ARCHITECTURE, AND DEVELOP A SECURITY RISK MANAGEMENT PLAN; MINIMUM EDUCATION/CERTIFICATION REQUIREMENTS : UNDERGRADUATE DEGREE IN COMPUTER SCIENCE, INFORMATION TECHNOLOGY, OR RELATED FIELD CISSP, CISM OR SIMILAR CERTIFICATION DESIRED. ---------- CONTRACT JOB DESCRIPTION Responsibilities: 1. Provides high-level architectural expertise to managers and technical staff. 2. Develops architectural products and deliverables for the enterprise and operational business lines. 3. Develops strategy of system and the design infrastructure necessary to support that strategy. 4. Advises on selection of technological purchases with regards to processing, data storage, data access, and applications development. Sets standards for the client/server relational database structure for the organization (Structured Query Language (SQL), Oracle, Sybase). 5. Advises of feasibility of potential future projects to management. Minimum Education/Certification Requirements : Bachelor’s degree in Information Technology or related field or equivalent experience

Client Information

Work Location:	OCTO - 200 I Street, SE Washington DC 20003	**Cost Center:**	OCTO - Office of the Chief Technology Officer

Required/Desired Skills

Required /Desired

Skill	Required /Desired	Amount	of Experience
16+ yrs as a Cyber Security Architect	Required	16	Years
16+ yrs building an IT system roadmap	Required	16	Years
Bachelor’s degree in Computer Science, Information Technology, or related field	Required	5	Years
Mastery level integration of Managed Security Services Providers (MSSP) and SIEM to support an enterprise environment	Required	5	Years
Experience in a role supporting, IT security, compliance, risk management and privacy, to include control selection	Required	5	Years
Experience implementing industry compliance and security standards (NIST CSF, PCI DSS, HIPAA)	Required	5	Years
Familiarity with archive, backup/recovery and business continuity processes in distributed operations	Required	5	Years
Significant knowledge of Application Security, Web Application, Information Security, Databases, Coding practice, and IT Infrastructure design	Required	5	Years
Experience with either CheckPoint or Palo Alto Firewalls	Required	5	Years
Experience with technology implementation/integration of perimeter tools: DDOS, Firewall, IPS/IDS, VPN, Threat Emulation	Required	5	Years
Experience with technology implementation/integration of endpoint tools: Vul Scanning, Endpoint Mangmt, Full Disk Encryption	Required	5	Years
Bachelor’s degree in IT or related field or equivalent experience	Required		

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 that will be used when submitting E-RTR.
Question 3	There are no reimbursable expenses. Do you accept this requirement?