Title:	OCIO Info. Assur./Sec. Spclt. Journeyman	**Region:**	District of Columbia
Req ID:	557311		

Details

Requisition Details

Req. Class:	IASSV1 : 2-Journeyman	**Region:**	District of Columbia
Title:	OCIO Info. Assur./Sec. Spclt. Journeyman		
Req. Status:	Open		
No. of Openings:	1	**No. Filled:**	0
Start Date:	04/30/2018		
No New Submittals After:	04/18/2018		
Max Submittals by Vendor per Opening:	4		

Worksite Address:	1101 4th Street SW suite w35
Agency Interview Type:	In Person
Advanced Technical Screening Required?:	No
Existing Incumbent Resource?:	No

Requisition Description

Engagement Type: Contract

Short Description: 6-10 years of experience. Determines enterprise information assurance and security standards.

Complete Description: As part of the OCFO technology team, the Security Specialist (Infrastructure Group) will be maintaining and monitoring day to day operation of the OCFO IT infrastructure – Security . The IT Consultant will help and performs, monitoring, maintenance, and security IT infrastructure (physical , virtual and cloud) . IT consultant will performs OS , security and application upgrades of servers and network to keep them up-to-date . IT consultant will develop, implements, maintains and enforces documented standards and procedures for the design, development, installation, modification, and documentation of assigned systems. IT consultant will plans, coordinates, and monitors project activities for OCFO Infrastructure group and duties as assigned. Experience with Windows 2008R2/2012/2012R2/2016 domain administration: (Active Directory Services (ADS), Group Policy, etc. Log analysis of Firewall , AD , Switches and other deployed security products Knowledge of Vulnerability assessment tools to identify and mitigate issues . Research, analyze, and patch required systems to comply with OCFO compliance mandates. Respond to escalation calls from the Help desk, Desktop support, and other teams to debug and resolve security and perform maintenance. Understands security troubleshooting processes and cooperates with other team . Assist Service Desk technicians as needed with Tier I and Tier II troubleshooting and patching of desktop systems, software (MS Office, Java, Adobe), printer issues, and server related issues as needed. Provides trouble-shooting assistance on production and non-production supported systems. May recommend methods and techniques for obtaining solutions. Initiates preventive maintenance the technical system. Good verbal and written communication and interpersonal skills Experience in producing and maintaining detailed step by step documentation. Security certification preferred (Security+ , CISSP other) --- CONTRACT JOB DESCRIPTION Responsibilities: 1. Determines enterprise information assurance and security standards. 2. Develops and implements information assurance/security standards and procedures. 3. Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' requirements. 4. Identifies, reports, and resolves security violations. 5. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. 6. Supports customers at the highest levels in the development and implementation of doctrine and policies. 7. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. 8. Performs analysis, design, and development of security features for system architectures. 9. Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers. 10. Designs, develops, engineers, and implements solutions that meet security requirements. 11. Provides integration and implementation of the computer system security solution. 12. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. 13. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. 14. Ensures that all information systems are functional and secure. Minimum Education/Certification Requirements: Bachelor's degree in Information Technology or related field or equivalent experience

Client Information

Work Location: OCIO - 1101 4th Street SW
Suite W350

Cost Center: OCIO - Office of the Chief Information Officer

Required/Desired Skills

Required /Desired

Skill	Required /Desired	Amount	of Experience
6-10 yrs developing, maintaining, and recommending enhancements to IS policies/requirements	Required	8	Years
6-10 yrs performing vulnerability/risk analyses of computer systems/apps	Required	8	Years
6-10 yrs identifying, reporting, and resolving security violations	Required	8	Years
Bachelor’s degree in IT or related field or equivalent experience	Required		
Patching Server 2008 / 2012 / 2016	Required	8	Years
Patching Desktop Windows 10 / 7	Required	8	Years
Firewall management CISCO NGFW	Required	8	Years
Vulnerability assessment tools Nessus , Tripwire	Desired	6	Years
VMware 5.5 / 6.0	Required	6	Years
Production support	Required	8	Years
Server and Desktop troubleshooting	Required	8	Years
NIST 800-53 experience	Desired	3	Years
Splunk	Desired	5	Years
Cloud experience (MS Azure)	Desired	2	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 that will be used when submitting E-RTR.
Question 3	There are no reimbursable expenses. Do you accept this requirement?