

Title: OCTO - Info. Assur./Sec. Spclst. **Region:** District of Columbia
Req ID: 591436

Details**Requisition Details**

Req. Class: IASSV1 : 2-Journeyman **Region:** District of Columbia
Title: OCTO - Info. Assur./Sec. Spclst.
Req. Status: Open
No. of Openings: 2 **No. Filled:** 1
Start Date: 06/24/2019 **End Date:** 09/30/2019
No New Submittals After: 06/07/2019

Worksite Address: 200 I St, SE Washington DC ;

Agency Interview Type: In Person

Advanced Technical Screening Required?: No

Existing Incumbent Resource?: No

Hours/Units per day: 8

Days per week: 5

Requisition Description

Engagement Type: Contract

Short Description: The Citywide Information Security (CWIS) team is looking for a senior Information Assurance specialist to work on Governance Risk and Control tasks.

Complete Description: 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

Work Location: OCTO - 200 I Street, SE
Washington DC 20003

Cost Center:

OCTO - Office of the Chief
Technology Officer

Project:

Required/Desired Skills

Required /Desired

Skill	Required /Desired	Amount	of Experience
6-10 yrs developing, maintaining, and recommending enhancements to IS policies/standards/procedures and writing System Security Plan (SSP)	Required	6	Years
6-10 yrs implementing Cybersecurity Risk Management Framework and/or Security Controls (NIST, ISO, CIS)	Required	6	Years
6-10 yrs identifying, reporting, and resolving security risks through audits and develop POAM's	Required	6	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.