

**Foxhole Technology**  
**CSMC, Leesburg, VA**

**Position Descriptions**

Personnel must meet the criteria in the job descriptions below to qualify for the positions under this contract

**Network Security Architect**

The Network Security Architect supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Network Security Architect is a member of the CERT Security Engineering Group.

This position requires the ability to:

- Identify technologies, tools, and deployment strategies to implement the critical elements of CSMC technology to secure our client's enterprise architectures. Provide overall direction, guidance and definition of our technical architecture to effectively support the CSMC's business strategy and increase operational efficiencies.
- Collaborate with stakeholders to establish and maintain and communicate a technical enterprise security roadmap. Assist in prioritizing network troubleshooting and maintenance and ensure that the CSMC technical infrastructure meet's CSMC's Service Level Agreements (SLAs).
- Develop implementation strategies, architectural designs, and recommendations for the best placement of network security devices such as IDS/IPS, tap, firewalls, etc.
- Plans, conducts and oversees highly complex projects or major phases of significant projects; Acts as a technical lead in security network engineering efforts
- Conducts investigations and tests of complex security software systems to enhance performance or investigate and resolve matters of significance
- Reviews completion and implementation of technical products to ensure success and timeliness
- Reviews literature, and current practices relevant to the solution of more complex network security projects
- Recommends corrections in complex technical applications and analysis to enhance performance
- Acts as the initial contact with vendors on more complex projects to provide required products or services
- Provides leadership and work guidance to less experienced personnel
- Provides technical consultation to other organizations; interacts with senior customer personnel and internal senior management
- Provides the customer base with first level support
- Performs comprehensive security assessment of all designs within all enterprise networks, advises senior level executives of network vulnerabilities, and develops procedures and polices to rectify
- Provide 24x7x365 application support (on-call responsibilities)

**Qualities/Additional info:** Network Security Architect should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent

interaction with government client is required. Occasional local travel. Occasional weekend hours (<10%) to support implementations & upgrades. Infrequent (<10%) long distance travel.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information systems
- Minimum ten years of relevant professional experience is considered equivalent to a Bachelor's degree

Experience:

- CISSP or GIAC/GSEC Certification
- CCNA, CCNP, or Network+ Certification
- Minimum ten years of Information Technology experience
- Minimum eight years of experience in network security engineering
- Experience with Enterprise Sensors (Sourcefire, SNORT, Cisco, ISS, McAfee, etc.)
- Experience with network principals, routers, switches, firewalls and VPN technologies
- Experience with full packet capture and DNS technology and concepts
- Strong networking background with clear understanding of network protocols, TCP/IP, LAN/WAN concepts
- Experience writing policies, procedures, and TTPs
- Experience composing presentations and briefing senior management

**Preferred Experience:**

- Experience with information security devices (e. g., firewalls, and intrusion detection/prevention systems) and applications (e.g. security information management tools like ArcSight)
- Experience with NAC and web proxy solutions (ForeScout, BlueCoat, etc.)
- Strong analytical and creative problem solving skills to resolve highly complex software design issues and create new software
- Good leadership skills to mentor, oversee, and lead team members
- Strong interpersonal skills to interact with senior customers, management and team members
- Strong communication skills to interact with team members and senior support personnel
- Experience working in a network security environment, such as a Security Operations Center (SOC), Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT), Computer Incident Response Center (CIRC) or Cyber Security Incident Response Center (CSIRC)

**Network Security Engineer**

The Network Security Engineer supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Network Security Engineer is a member of the CERT Security Engineering Group.

This position requires the ability to:

- Plans, conducts and oversees highly complex projects or major phases of significant projects; Performs security network engineering efforts
- Conducts investigations and tests of complex security software systems to enhance performance or investigate and resolve matters of significance
- Reviews completion and implementation of technical products to ensure success and timeliness
- Reviews literature, and current practices relevant to the solution of more complex network security projects

- Recommends corrections in complex technical applications and analysis to enhance performance
- Acts as the initial contact with vendors on more complex projects to provide required products or services
- Provides leadership and work guidance to less experienced personnel
- Provides technical consultation to other organizations; interacts with senior customer personnel and internal senior management
- Provides the customer base with first level support
- Performs comprehensive security assessment of all designs within all enterprise networks, advises senior level executives of network vulnerabilities, and develops procedures and policies to rectify
- Provide 24x7x365 application support (on-call responsibilities)

**Qualities/Additional info:** Network Security Engineer should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<10%) to support implementations & upgrades. Infrequent (<10%) long distance travel.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information systems
- Minimum ten years of relevant professional experience is considered equivalent to a Bachelor's degree

Experience:

- CISSP, CCNA, Security+ and/or relevant Certification
- Minimum eight years of experience in network security engineering, network security analysis or OS programming
- Minimum six years of Computer Network Defense (CND) experience
- Experience with Enterprise Sensors (Sourcefire, SNORT, Cisco, ISS, McAfee, etc.)
- Experience with IDS/IPS custom signature creation and deployment
- Experience with full packet capture and DNS technology and concepts
- Experience with network principals, routers, switches, firewalls and VPN technologies
- Experience writing policies, procedures, and TTPs
- Experience composing presentations and briefing senior management

**Preferred Experience:**

- Development experience with a programming language, especially the following: C, C++, Java, with additional familiarity in languages such as Ruby, Perl, Python, and SQL
- Experience with information security devices (e. g., firewalls, and intrusion detection/prevention systems) and applications (e.g. security information management tools like ArcSight)
- Experience with NAC and web proxy solutions (ForeScout, BlueCoat, etc.)
- Strong analytical and creative problem solving skills to resolve highly complex software design issues and create new software
- Good leadership skills to mentor, oversee, and lead team members
- Strong interpersonal skills to interact with senior customers, management and team members
- Strong communication skills to interact with team members and senior support personnel
- Experience working in a network security environment, such as a Security Operations Center (SOC), Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT), Computer Incident Response Center (CIRC) or Cyber Security Incident Response Center (CSIRC)

## **Network Engineer**

The Network Engineer is filled by an individual skilled in the area of network and hardware support. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Network Engineer is a member of the CERT Infrastructure Group.

This position requires the ability to:

- Maintain all network devices which may include, but not limited to, switches (including VOIP), hubs, cables, routers, and firewalls
- Configuration management which includes thorough documentation of all network/hardware changes
- Provide recommendations to government personnel on performance tuning and hardware enhancements
- Must have hands-on knowledge of router and switch configurations (LAN, WAN, VLAN)
- Monitor health and welfare of all network hardware equipment
- Develop Life Cycle plan for all network devices in support of infrastructure
- Maintain connections between primary, secondary, and back-up sites
- Assist with troubleshooting in regards to network connectivity
- Assist government staff with requirements development and prepare evaluation/testing criteria for proposed new equipment as needed
- Provide 24x7x365 application support (on-call responsibilities)

Qualities/Additional info: Network Engineer should be prepared to take on the duties of network design and configuration policy deployment. Candidate should understand the use of service networks and multi-tiered DMZs in a LAN/WAN topology.

The candidate will have professional experience in designing, deploying, and troubleshooting routed networks using Cisco Routers as well as layer-2 and layer-3 switching products. The candidate has experience with internal, Extranet, and public Internet connections delivered via a variety of carrier facilities (point to point circuits, MPLS, Frame Relay, Ethernet, etc.).

Additionally, the ideal candidate is proficient in working with Cisco routing equipment in an environment encompassing private internal networks, customer and business partner Extranet connectivity, and multi-homed Internet connectivity.

Network Engineer should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<5%) to support implementations & upgrades. Infrequent (<5%) long distance travel.

### **Required Education and Experience:**

#### Education:

- Bachelor's degree in Computer Science or Information systems

- Minimum ten years of relevant professional experience is considered equivalent to a Bachelor's degree

Experience:

- In addition to required education or equivalent experience:
- Minimum six years of technical network administration experience
- CISCO CCNA or CCNP Certification
- Experience with network switches and routers, e.g., Cisco products and VOIP technology
- Experience providing end-user support in a Help Desk or WAN NOC environment
- Written and oral communications skills

**Preferred Experience:**

- Experience with enterprise firewall and VPN administration
- Experience with enterprise VPN endpoint deployments and architecture
- Experience with business process reengineering, capability maturity model, change management, or process improvement
- Experience with information security devices (e. g., Cisco, F5, ForeScout, LAN/WAN, etc) and applications (e.g. security information management tools like ArcSight)

## **Firewall Engineer**

The Firewall Engineer is filled by an individual skilled in the area of firewall and network security support. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Firewall Engineer is a member of the CERT Infrastructure Group.

This position requires the ability to:

- Maintain all firewall and VPN devices which may include, but not limited to, Juniper firewalls, Juniper NSM management appliance, Juniper VPN devices, cables, and Cisco ASA firewalls
- Configuration management which includes thorough documentation of all network/hardware/firewall changes
- Provide recommendations to government personnel on performance tuning and hardware enhancements
- Must have hands-on knowledge of firewall and VPN configurations
- Must have solid background on LAN/WAN/networking concepts
- Monitor health and welfare of all firewall and VPN networking equipment
- Develop Life Cycle plan for all network device in support of infrastructure
- Maintain connections between primary, secondary, and back-up sites
- Maintain connections between CSMC and its customers
- Support Security Engineering Group with FAS implementation in regards to firewall and VPN connectivity
- Assist government staff with requirements development and prepare evaluation/testing criteria for proposed new equipment as needed
- Provide 24x7x365 application support (on-call responsibilities)

Qualities/Additional info: Firewall Engineer should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<5%) to support implementations & upgrades. Infrequent (<5%) long distance travel.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information systems
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree

Experience:

- In addition to required education or equivalent experience:
- Minimum five years experience in enterprise firewall and/or VPN administration
- Minimum five years technical network administration experience
- CISSP, CISCO CCNA, Security+ and/or relevant Certification
- Experience with network firewalls, switches, and routers, e.g., Cisco and Juniper products
- Experience with enterprise VPN endpoint deployments and architecture
- Experience with Juniper Network and Security Manager (NSM)
- Experience with firewalls, e.g., Cisco ASA and Juniper Netscreen
- Experience providing end-user support in a Help Desk or WAN NOC environment
- Written and oral communications skills

**Preferred Experience:**

- Experience with business process reengineering, capability maturity model, change management, or process improvement
- Experience with information security devices (e. g., Cisco, F5, ForeScout, LAN/WAN, etc) and applications (e.g. security information management tools like ArcSight)

## **Storage Area Network (SAN) Engineer**

The Storage Area Network Engineer is filled by an individual skilled in the area of storage area network support. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Storage Area Network Engineer is a member of the CERT Infrastructure Group. This position requires the ability to:

- Plan, design, install, and maintain storage systems in multiple data centers
- Handle the tasks of troubleshooting storage related issues in a variety of environments
- Understand storage protocols including ISCSI, Fiber Channel, NFS and hardware, which uses these protocols
- Install, set up, and maintain backup and storage area network environment
- Understand routing principles, design of consistent network-wide file system layouts and client/server programming
- Maintain all storage devices which may include, but not limited to disk array units, fiber switches, cables
- Manage configuration of storage infrastructure and document changes
- Monitor health and welfare of all storage equipment by analyzing system logs
- Develop Life Cycle plan for all storage devices in support of infrastructure
- Maintain storage backups at primary, secondary, and/or back-up sites
- Support System Administrator with back-up troubleshooting in regards to network and disk space
- Provide recommendations to government personnel on performance tuning and hardware enhancements
- Assist government staff with requirements development and prepare evaluation/testing criteria for proposed new equipment as needed
- Provide 24x7x365 application support (on-call responsibilities)

Qualities/Additional info: Storage Area Network Engineer should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should

also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<5%) to support implementations & upgrades. Infrequent (<5%) long distance travel.

### **Required Education and Experience:**

#### Education:

- Bachelor's degree in Computer Science or Information systems
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree

#### Experience:

- In addition to required education or equivalent experience:
- MCSE, CCNA, Security+, and/or relevant Certification
- Minimum five years experience in handling storage infrastructure
- Experience with DAS, SAN, and NAS concepts, snapshots, clustering, mirroring, fail-over, file permission management, and disaster recovery
- Experience with managing large storage environments (32 TB or larger)
- Experience with storage equipment, e.g., EMC, NetApp, Compellent products
- Experience with Windows and Linux OS administration
- Knowledge of router and switch configurations (LAN, WAN, VLAN)

### **Preferred Experience:**

- SCP, SCSE, SCA, or SCSN-E Certification
- Experience with business process reengineering, capability maturity model, change management, or process improvement
- Experience with security information management tools like ArcSight

### **Program Manager**

The Program Manager supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia. OSEM responsibilities include:

- The Program Manager will take direction from the CERT Director and/or Contracting Officer's Technical Representative (COTR) for all work to be performed by Contract personnel.
- Serve as the on-site contact for contractor personnel understanding the latest status of projects being worked by the contractor team, handling scheduling of personnel, drafting reports, and being the first line of communication with the Agency concerning contractor team issues.
- Build, oversee, grow and support as necessary, the CERT Operations and Support Teams consisting of:
  - The Protection Group performing Network Mapping, Vulnerability Assessment, Antivirus protection, etc.
  - The Detection Group performing:
    - 1<sup>st</sup> level analysis of network traffic using Intrusion Detection/Prevention Sensors (IDS/IPS) sensors.
    - 2<sup>nd</sup> level analysis of network traffic using IDS/IPS sensors and a Security Information Management (SIM) tool.
    - Maintenance, security control configuration and rule set development for various security devices.
  - The Response Group coordinating activities with field site personnel as directed by the government.

- The Development Group performing research, testing, implementation, configuration and maintenance functions.
- The Infrastructure Group performing Information Security asset deployments, as well as database, network, system and firewall administration functions.
- Set up and maintenance of research and development lab, including cradle-to-grave assessments of potential new tools for incorporation into the security architecture
- Recommend technological/architectural upgrades/modifications to Agency information security architecture
- Serve as a technical resource at Agency meetings and presentations
- Provide input to draft InfoSec policies
- Augment coverage for shifts positions when required

Qualities/Additional info: Program Manager should be a proven team player with excellent oral and written communications skills and the ability to work in high pace / demanding environment with technical staff implementing processes and procedures and senior / executive customer staff at an agency policy level. Program Manager should also be a self-starter, capable of working projects cradle-to-grave, independently if necessary. Continuous interaction with government client is required. Occasional local travel. Infrequent (<5%) long distance travel.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information systems.
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree.
- Qualified candidates must have a minimum of one year experience managing a CSIRC type operation for a government or commercial client with a staff of at least 25 persons.

Experience:

- In addition to required education or equivalent experience;
- Minimum 12 years IT experience with at least five years in Network Security.

**Preferred Experience:**

- Three years network security analysis, using intrusion detection systems.
- Experience with vulnerability assessment tools (Nessus, FoundScan, etc.)
- Experience conducting analysis at the packet level.
- Experience working in a network security environment, such as a Security Operations Center (SOC), Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT), Computer Incident Response Center (CIRC) or Cyber Security Incident Response Center (CSIRC).
- Experience with Capability Maturity Models (CMM)
- Firewall administration experience (Checkpoint, etc.)
- Experience with Snort, ISS and Cisco intrusion detection sensors.
- Experience with Host-Based and Network-Base IDS
- Experience with Security Information Management Tools (ArcSight, netForensics, e-Security, etc.)
- AntiVirus, AntiSpyware, and Content Filtering solutions
- Help Desk Systems and Network Management solutions

CISSP and/or SANS/GIAC Certification

### **3.5.2 Systems Analyst**

The Systems Analyst is filled by an individual skilled in the area of IT technical writing and reporting. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Systems Analyst is a member of the Program Management Office (PMO). The primary focus of the PMO is to apply best practices to projects directly supporting CERT operations. The Systems Analyst contributes to soliciting client stakeholder participation in project development and execution as well as status of ongoing service delivery. The Systems Analyst is responsible for the following duties:

- Work with project stakeholders and system users to capture the FAA CSMC operational business process models within MS Visio and the WebSphere Business Modeler tool.
- Facilitate information gathering sessions with key CSMC personnel for process and business requirement elicitation and documentation
- Focus on providing key insight to the development of the technology solutions to meet the needs of CSMC's personnel and their clients
- Develop and run simulation scenarios on baseline models with an emphasis on identifying constraints, bottlenecks, and opportunities for optimization where applicable
- Capture dynamic analysis data on simulation results packages and format data into reports accordingly
- Perform comparison analysis on baseline (As-Is) and future (To-Be) process models emphasizing the key efficiencies and deficiencies with each model.
- Iteratively analyze the people, process, and technology impacts of the CSMC's core operational processes.
- Drive efficiency within CSMC's on site development activities through providing a disciplined SDLC methodology
- Institute and maintain best practices for documentation and delivery for all on site software development

### **Facilities Representative**

The Facilities Representative supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Facilities Representative will take direction from the Contracting Officer's Technical Representative (COTR) for work to be performed to support the physical plant of the CSMC. Serve as the on-site contact for contractor personnel understanding the latest status of projects being worked by the contractor team, handling scheduling of personnel, drafting reports, and being the first line of communication with the Agency concerning contractor team issues.

- Must be able to work with Facility Management Personnel

- Must have experience working with Facility Power systems, HVAC systems, Internet and Telco Connectivity, and Fire protection systems installed in Computer Operations Facilities.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information systems.
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree.

Experience:

- In addition to required education or equivalent experience;
- Minimum 8 years IT experience with at least three years in Network Security.

**Senior Associate Client Account Representative (ACAR)**

See 3.5.5 ACAR. Bachelor's Degree is required.

**Associate Client Account Representative (ACAR)**

The Client Account Representative position is filled by an individual skilled in the area of cyber security service delivery and client relations. This position supports an Information Systems Security Line of Business (ISS LOB) Shared Service Provider (SSP) for Situational Awareness and Incident Response (SAIR) performing cyber security functions protecting the network security of tens of thousands of users for multiple Federal clients. The work site is located in Leesburg, VA.

The Client Account Representative is a member of the Program Management Office (PMO). The primary focus of the PMO is to apply Project Management Body of Knowledge (PMBOK) best practices to projects directly supporting CERT operations. The Client Account Representative contributes to soliciting client stakeholder participation in project development and execution as well as status of ongoing service delivery. The Client Account Representative is responsible for the following duties:

- Communicates client needs to the organization to promote alignment of the evolution of organizational capabilities and services with those needs; gathers requirements from clients to identify potential service enhancements
- Conducts regular interaction with clients to maintain open communications to ensure satisfactory service delivery
- Contributes to the development and updating of Service Level Agreements (SLAs), Memoranda of Agreement and/or Understanding (MOA/MOU), etc.
- Manages the implementation process for new client on-boarding
- Tracks the status of client correspondence and SLA performance throughout the life of the client service period
- Coordinates with Operations and Infrastructure teams to address status and manage resolution of client issues
- Interfaces with technical and non-technical personnel, ensuring the development of integrated solutions that meet client needs and manage expectations

Qualities/Additional Info: Candidate should be a proven team player with fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Strong oral and written communications skills are a must in

order to effectively interact with clients up to and including executives at the CIO and CISO level. Familiarity with NIST standards and OMB guidelines as applicable to cyber security is required. Frequent interaction with Government client is required. Occasional local travel. Infrequent (<5%) long distance travel.

### **Required Education and Experience:**

#### Education:

- Bachelor's degree in Computer Science or Information Systems
- Minimum four years of relevant professional experience is considered equivalent to a Bachelor's degree.

#### Experience:

In addition to required education or equivalent experience:

- Minimum four years IT experience.
- Two years' experience in the role of or working directly with cyber security personnel.
- Must be familiar with Microsoft Office Suite (including Word, Excel, PowerPoint, Visio, and Project).

### **Preferred Experience:**

- Experience in a Security Operations Center (SOC) or CERT
- Incident handling and response, network security analysis, intrusion detection systems, firewalls, and/or Security Information Management

Relevant professional certifications: ITIL V3, Security+, CISSP, GIAC

### **3.5.6 Intermediate Associate Client Account Representative (ACAR)**

See 3.5.5 Senior ACAR. Bachelor's degree is not required. Minimum two years IT experience.

### **C&A Specialist**

The Certification & Accreditation Specialist (C&A) is filled by an individual skilled in the area of NIST 800-53A and FAA 1370.82A. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The C&A Specialist is a member of the CERT Administration Group (AG). The primary focus of the AG is to support management and assist with the daily activities of running a CERT. The C&A Specialist is responsible for:

- Authoring Certification & Accreditation Document, such as:
  - Vulnerability Assessments
  - Risk Assessments
  - Information System Security Plans
  - Contingency/Disaster Recovery Plans
  - Security Test and Evaluation Plans and Reports
  - Plan of Actions & Milestones (POA&Ms)
  - Signature Pages, Executive Summaries, etc.
- Performing C&A Testing

Qualities/Additional info: C&A Specialist should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Extremely effective oral and written communications skills are a must, in order to present strategy, scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<5%) to support implementations & upgrades. Infrequent (<5%) long distance travel.

### **Required Education and Experience:**

#### Education:

- Bachelor's degree in Computer Science or Information systems.
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree.

#### Experience:

- In addition to required education or equivalent experience;
- Minimum six years IT experience with at least three years experience in the role of C&A
- Must be familiar with NIST 800-53A and FAA 1370.82A.

### **Preferred Experience:**

Experience with business process reengineering, capability maturity model, change management, or process improvement.

### **Senior II Technical Writer**

The Senior Technical Writer (2) is filled by an individual skilled in the area of IT technical writing and reporting. This position supports a Civilian Agency Computer Emergency Response Team (CERT) organization protecting the network security of tens of thousands of users. The work site is located in Leesburg, Virginia.

The Senior Technical Writer is a member of the CERT Administration Group (AG). The primary focus of the AG is to support management and assist with the daily activities of running a CERT. The Senior Technical Writer is responsible for: Editing, writing, and/or rewrites technical articles, publications, presentations, and other materials to communicate clearly and effectively research findings, technical developments, and other news and information to a wide range of external audiences. Interprets and administers documentation/ communication policies and procedures. Advises writers and researchers in matters of style, syntax, and usage to improve the general quality and effectiveness of communications. Exercises quality control over documents intended for external distribution. May participate in copy clearance process.

The Senior Technical Writer regularly contributes to the development of new concepts, techniques, and standards. Considered expert in field within the organization.

Qualities/Additional info: Senior Technical Writer should be a proven team player with excellent oral and written communications skills, and a fine attention to detail. He/she should also be a self-starter, capable of working on projects independently, if required. Effective oral and written communications skills are a must, in order to present strategy,

scripting output and status information to the client in both formal and informal review settings. Frequent interaction with government client is required. Occasional local travel. Occasional weekend hours (<5%) to support implementations & upgrades. Infrequent (<5%) long distance travel.

**Required Education and Experience:**

Education:

- Bachelor's degree in Computer Science or Information Systems.
- Minimum six years of relevant professional experience is considered equivalent to a Bachelor's degree.

Experience:

- In addition to required education or equivalent experience;
- Minimum six years IT experience.
- Must have least three years' experience in the role of Technical Writer.
- Must be familiar with: Microsoft Office & Project.

**Preferred Experience:**

Experience with business process reengineering, capability maturity model, change management, or process improvement.

-