SARAH SMITH
Address, City ST 00000 United States
Tel.: 000-000-0000; email: name@email.com

Vacancy #: DE-00000000-00-CAS
IT SPECIALIST, DEPARTMENT OF THE NAVY

PROFESSIONAL SUMMARY

Motivated, solutions-focused, and trusted 8570-compliant Information Technology (IT) professional with a decade of government contractor experience in cybersecurity, vulnerability management, HBSS (McAfee), ACAS (Nessus), STIG compliance, DIACAP and RMF validating. Expert in DOD frameworks, Command Cyber Readiness Reviews (CCRRs), and Assessment & Authorization (A&A) Reviews. Experienced in team leadership, IT management, system performance, problem-solving, policies and procedures, applications software, operating systems, network services, data management, systems administration, customer support, planning, enterprise architecture, information security, cybersecurity, and systems analysis. Demonstrated success as a creative, innovative thinker, fostering executive management trust and acclaim, leading to additional responsibility and promotions. Astute developer of policies and procedures to ensure information systems reliability and accessibility and to prevent and defend against unauthorized access. Expert in conducting risk and vulnerability assessments of planned and installed information systems, participating in network and systems design to ensure implementation of appropriate systems security policies, and assessing security events to determine the impact and implementing corrective actions.

Skilled in customer support, information assurance, software testing and diagnostics, desktop services, network troubleshooting, evaluation, monitoring, security patches, standard operating procedures, performance standards, penetration testing, technical guidance, information assurance control validation, software registration, performance metrics, metrics analysis, resource management, IT principles and concepts, diverse IT operational requirements, IT policies and processes, technical resources planning, relationship building, and communication. Outstanding abilities in customer service, professionalism, and fostering teamwork. Superior capacity to solve complex problems involving a wide variety of information systems; able to work independently on large-scale projects, and thrive under pressure in fast-paced environments while directing multiple projects from concept to implementation. Strong team and relationship building skills.

PROFESSIONAL EXPERIENCE

00/2000 to Present, ***SENIOR CONSULTANT,*** Company, address, City ST 00000, 40+ hours per week, $000,000 per year, supervisor: Name, 000-000-0000, may contact.

INFORMATION SECURITY RISK SPECIALIST. Perform Cyber Command Readiness Inspections (CCRI) reviews of Host Based Security Systems (HBSS) and Microsoft Windows on Department of Defense (DoD) Information Systems. Consult with company leaders and client organizations to discover cyber risks, understand applicable policies, and develop mitigation plans. Work with

technical, environmental, and personnel details from Subject Matter Experts (SMEs) to assess the entire threat landscape. Guide clients through a plan of action with presentations, white papers, and milestones. Translate security concepts for clients, so they can make the best decisions to perform Cyber Command Readiness Inspections (CCRI) reviews of the host-based security system (HBSS) on DoD information systems.

IT CYBERSECURITY MANAGEMENT. Perform system security reviews/audits and Certification & Accreditation (C&A)/Assessment and Authorization (A&A) utilizing eMASS, ACAS, and HBSS. Assist with development and tracking of the Plan of Action and Milestones (POA&M) in eMASS. Conduct A&A process for IT systems and networks following the DoD Risk Management Framework (RMF) process. Review and approve test and evaluation activities to validate those threats and vulnerabilities are mitigated.

CYBERSECURITY THREAT ANALYSIS. Analyze and review results of network and system vulnerability scans and validate implementation of Information Assurance (IA) controls per DoD 8500. Supervise, plan, administer, manage, operate, integrate, secure, and troubleshoot information systems, local area networks (LANs), and enterprise services. Guide personnel on interoperability, integration, and security of networks. Advise other IT Specialists and staff concerning system level errors. Utilize IT principles, concepts, and methods regarding data storage, software applications, and networking. Define strategies to identify and improve implementation as it relates to the network, systems, devices, and access for regulatory and compliance requirements. Safeguard cabling, wireless, switching, and security systems.

DOD CERTIFICATION & ACCREDITATION. Oversee Department of Defense (DoD) Cybersecurity Certification and Accreditation (C&A), Authorization and Assessment (A&A), and Authority to Operate (ATO) processes. Perform validation for DISA RMF packages. Use DoD Risk Management Framework and associated NIST documents. Support the Program Manager, SCAL, ISSM, and ISSE throughout all phases of the security authorization process.

IT TEAM LEADERSHIP. Work as part of a dynamic technical travel team to assess the security posture of HBSS assets in CONUS and OCONUS locations. Collaborate on team assignments, projects, problem to be solved, actionable events, milestones, program issues under review, and deadlines and timeframes for completion. Communicate the organization's overall strategic plan. Guide new and existing Cybersecurity professionals for training and certification. Offer escalated support for high-priority requests or complex technical problems. Mentor and advise other specialists on IT systems and provide on-the-job and formal training. Cross-train for understanding and assistance with server, security, and network functionality, use, and troubleshooting techniques.

ASSESS, DETERMINE, AND TROUBLESHOOT CYBERSECURITY. Review security and operations in cyberspace. Encompass a full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery activities. Address computer network operations and performance, and information assurance. Maintain network security to be proactive against malicious inside and outside threats. Ensure computers in Disaster and Recovery rooms comply with IT security policies. Cooperate with network administrators and security analysts for complex issue resolutions regarding rogue devices, persistent malware, and other

issues of cybersecurity. Create, change, and delete user accounts per request to ensure efficiency, user protection, and network access. Administer hard drive sanitization and provide IT Security certificate of sanitization or destruction upon completion. Develop and recommend improvements to inspection, evaluation, and penetration testing methodologies for cybersecurity appraisals. Perform various security assessments using DoD Security Technical Implementation Guides (STIG) and DISA Security Content Automation Protocol (SCAP) compliant tools on various technologies to include Network, UNIX, and Windows-based programs and technologies.

ATTENTION TO DETAIL, COMMUNICATION, CUSTOMER SERVICE, AND PROBLEM SOLVING. Diagnose IT issues to provide customer support, technical advice, guidance, and recommendations. Plan delivery of IT customer support services, to include hardware and software installations, configuration, and troubleshooting. Present systems analysis observations to senior leadership to make recommendations. Communicate software and hardware problems to support staff or managers to discuss appropriate actions. Attend conferences, meetings, or presentations to discuss technical matters related to managed programs.

KEY ACCOMPLISHMENTS

- *Completed multiple whitepapers. As Project Lead, gather input from other project members and compile recommendations for improvements to the process and how those processes would save time, reduce cost, and help improve client relations. The changes were reviewed and implemented by the management team.*
- *Teach training classes and train junior team members on Microsoft Windows and EPS/HBSS.*
- *Praised as "extremely knowledgeable and thorough during the inspection process. The level of professionalism and positive attitude demonstrated by Sarah is by far the best we have ever encountered during a CCRI."*

00/2000 to 00/2000, ***PRINCIPAL INFORMATION ASSURANCE SPECIALIST/HBSS ADMINISTRATOR (PROMOTED TO TEAM LEAD),*** Company Corp., contractor for Naval Information Warfare Systems Command (NAVWARSYSCOM, formerly SPAWAR), City Data Center, US Navy, City ST 00000, 40+ hours per week, $000,000 per year, supervisor: Name, 000-000-0000, may contact.

TECHNOLOGICAL EXPERTISE. Ensured daily maintenance and secure operation of all unclassified systems within Millington Data Center to include all network, storage, and virtual machines (700 + systems & devices). Implemented and enforced IS security policies, assisted with development of system certification documentation, and responded to security incidents. Performed monthly STIG/Vulnerability compliance scans using SCAP, McAfee HBSS, and ACAS to verify DoD compliance. Performed all Operating System vulnerability patching.

VULNERABILITY AND THREAT ASSESSMENTS. Performed weekly vulnerability assessments to determine open Information Assurance Vulnerability Alerts (IAVAs). Reviewed and evaluated the security posture of computer system configurations, identified deficiencies and actions needed to correct deficiencies. Performed system security reviews/audits and Certification & Accreditation (C&A)/Assessment and Authorization (A&A) utilizing eMASS, ACAS, and Host-Based Security System (HBSS). Installed and configured operating tools for identification of software

vulnerabilities that support the development, integration, test, and evaluation of networking systems: ACAS, HBSS, SCAP, STIGs and Benchmarks, STIG Viewer eMASS and performed vulnerability scanning on Windows Server 2003, 2008/R2, 2012, Red Hat Linux, CentOS, and IBM AIX.

STRONG COMMUNICATIONS SKILLS TRANSLATING TECHNICAL TO LAY LANGUAGE AND AUDIENCES. Utilized excellent communication skills to convey ideas and technical approaches in easy-to-understand terms to enable strong decision-making. Briefed data center leadership on security posture, vulnerability management, metrics, and compliance. Disseminated written reports and status updates that were factual, timely, and error-free. Communicated, explained, and defended ideas and information clearly. Listened to others to identify alternatives to solve technical problems. Provided Authorization and Assessment (A&A) and reaccreditation of applicable systems per RMF/DIACAP.

COLLABORATION AND COOPERATION. Worked closely with Application, Network, and Systems Administrators to implement DoD mandated compliance STIGS and IAVAs/vulnerabilities. Engaged with leadership daily (NRC, NPC, BUPERS & SPAWAR IAM's) to maintain acceptable levels of compliance.

IT, IS, AND CYBERSECURITY MANAGEMENT. Administered the HBSS tools to include maintaining McAfee ePO server, monitoring agents, creating and adjusting firewall settings, reviewing logs, installing and removing agents and modules, and policy auditor. Administered ACAS Server performing vulnerability scanning on Windows Server 2003, 2008/R2, 2012, Red Hat Linux, CentOS, and IBM AIX. Performed STIG validations on IT assets to include Windows 2003, 2008/R2, 2012/R2, Member Servers, and Domain Controllers. Performed full STIG assessments through documentation; identified and documented the audit findings on the physical and virtual servers, switches, and storage in a standard report format, and completes and delivers the STIG assessment documentation. Conducted daily, weekly, and monthly network vulnerability scanning to determine and maintain enterprise compliance. Troubleshot and maintained cybersecurity operating systems and software applications and performed daily maintenance and secure operation of all unclassified and classified systems within Millington Data Center to include all network, storage and virtual machines (700 + systems & devices).

TEAM LEADERSHIP. Managed interdisciplinary project teams to ensure IA software packages, patches, security updates, and custom scripts to review system capabilities of 700+ servers within the SPAWAR Millington Data Center using Lumension Patch and Remediation.

KEY ACCOMPLISHMENTS

- *Performed complete rebuild and configuration for all IA tech refresh systems to include HBSS, SCAP, and Lumension. The complete rebuild included design, implementation (OS & Application), configuration, testing of IA tools. Responsible for the roll-outs of all agents and modules of DEV, TEST, and PROD for 13 different domains (500+ systems).*
- *Responsible for the complete rebuild and confirmation of the City disaster recovery site IA tools to include HBSS, SCAP, Lumension & ACAS.*

- *Managed and deployed Information Assurance (IA) software packages, patches, security updates, and custom scripts to 700+ servers in the SPAWAR Millington Data Center using Lumension Patch and Remediation.*
- *Created POA&Ms for IT Operations to drive down the number of open IAVAs.*

00/2000 to 00/2000, ***SYSTEMS ADMINISTRATOR*****,** Company Corp., contractor for Navy Recruiting Command), City ST 00000, 40+ hours per week, $000,000 per year, supervisor: Name, 000-000-0000, may contact.

IT SYSTEMS TECHNICAL PROFICIENCY. Responsible for the security posture of all virtual systems located in the eDMZ (Millington DATA Center), 120 + systems and network devices. Performed weekly STIG compliance scans using Retina, SCAP, McAfee HBSS & ACAS to verify DoD compliance and weekly vulnerability assessments to determine open IAVMs. Worked closely with Application, Network, and Systems Administrators to implement DoD-mandated compliance STIGS and IAVAs/vulnerabilities. White-listed applications and responsible for security baselines, troubleshooting HBSS firewall and IPS related issues, building exceptions and rules for valid network traffic. Reviewed ACAS vulnerability assessments and implemented necessary patching/STIGing to meet compliance standards.

APPLICATION DEPLOYMENTS. Performed Application Deployments to the DEV, TEST & Production Environments. Used systems administrator tools daily to include Active Directory, IIS, Cisco devices (Routers & Switches), Lumension, HBSS, F5 BIG IP. Systems Administrator for NRC's Macintosh (Apple) network. Completed OS redesign to implement DOD mandated STIGs and vulnerability patches for all Apple servers and workstations.

00/2000 to 00/2000, ***PROJECT/FIELD ENGINEER*****,** Company, address, City ST 00000, 40+ hours per week, $000,000 per year, supervisor: Name, 000-000-0000, may contact.

IT EXPERTISE AND PROCESS IMPROVEMENT. Provided senior-level technical IT consulting services for PCs, cabling, network, telephony, printers, Wi-Fi, peripherals, and audio/visual. Installed new hardware, systems, and software for existing and new networks. Provided end-user VPN support, personal device security, developed and implemented data backup and disaster recovery plans. Troubleshot PC hardware, printers and drivers, programming account tracking and reports, routers and switches, and firewall. Developed custom scripts and tools to solve workflow stalls or to improve production. Installed LAN services. Recommended revisions or improvements on planned systems. Coordinated directly with customers and technical representatives to plan, coordinate, and advise on current and planned work.

EDUCATION

Bachelor of Arts in Applied Science/Data Communications System Technology, University, City ST, 2000, 0.00 GPA; 120 semester hours; Class Valedictorian

Associate of Science, Applied Science/Computer Network Systems, University, City ST, 2000, 0.00 GPA, 68 semester hours, Class Salutatorian

OTHER

US Citizen
Top Secret/SCI Security Clearance

CERTIFICATIONS AND TRAINING

- MCITP Server Administration
- Security + - CompTIA
- Lean Six Sigma
- Certified HBSS Administrator (DOD)
- Certified ACAS Administrator (DOD)
- AWS Certified Solutions Architect
- Microsoft Certified Professional ID# 0000000
- Microsoft Certified Solutions Associate
- Microsoft Certified Professional
- Microsoft Certified Technology Specialist
- Microsoft Certified IT Professional
- ACAS SRR Training Class with Cert
- HBSS 201 & 301 Training
- HBSS SRR Training Class with Cert
- Windows SRR Training Class with Cert
- Windows Web / Database SRR Training Class with cert
- RMF SRR Training class with cert
- eMASS v5.5 SRR with cert
- Security + with CEs ID
- 2000 FY20 Cyber Awareness Challenge
- 2000 FY20 Personally Identifiable Information Training
- 2000 FY20 Phising ver 4.0
- 2000 FY20 Annual Security Awareness
- 2000 FY20 Derivative Classification
- 2000 FY20 Insider Threat
- 2000 FY20 Level 1 Antiterrorism
- 2000 FY20 SEER Training

AFFILIATIONS

XYZ in Technology
Tech Excellence for XYZ Group