Marcia Johnson

Project Manager (PM) - Computer Sciences Corporation (Assignments)

Pittsboro, NC - Email me on Indeed: indeed.com/r/Marcia-Johnson/5c81e2b329f5d473

Over 25 years of experience in the area of Information Technology infrastructure and support and an expert in Assessment and Authorization (formerly Certification and Accreditation) processes. An accomplished program/project manager and has been responsible for high-visibility deliverables. Dr. Johnson is thorough and conscientious in attention to detail, displaying strong leadership and interpersonal skills in managing employees, subcontractors, and vendors. Broad experience in directly interfacing with customers in the Commercial, Law Enforcement, DoD, and Intelligence communities.
Willing to relocate: Anywhere
Authorized to work in the US for any employer

WORK EXPERIENCE

Project Manager (PM)

Computer Sciences Corporation (Assignments) - April 2007 to August 2016

Assigned as the Project Manager on Confident ID Mobile, Multi-Factor Authentication, and Business Continuity and Disaster Recovery Projects. Previously assigned to the AppSEC on Demand Project Team. AppSEC on Demand tests the security of software and helps clients build security into the development process. Has presented the project to both upper management and at technical conferences. Previously assigned as the Project Manager for the Security Strategy Roadmap, Security Accountability Scorecard, and Separation of Duties projects. Creates and implements project definitions, schedules, and objectives. Works with stakeholders through workshops, meetings, email and phone calls to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations. Facilitates project team members to ensure communication and understanding of deadlines, assignments, and objectives. Reports and performs ongoing review of project status and identifies possible project risks. Recommends and implements risk mitigation solutions as approved and as appropriate. Addresses performance issues within prescribed guidelines.

Information Assurance Representative

Computer Sciences Corporation (Assignments) - July 2011 to September 2011

Served as a senior representative for the Defense Information Systems Agency (DISA) as the Information Assurance (IA) Representative to the U.S. Special Operations Command (USSOCOM). Assigned to USSOCOM's IA, Network Defense Group as the DISA Field Security Office (FSO) liaison for all DISA IA issues. Synchronized and provided technical expertise and customer advocacy to USSOCOM to improve use of and satisfaction with DISA-provided systems and services. Proactively communicated with the customers to understand requirements and gain their support. Performed Site Assistance Visits (SAVs) in preparation for Command Cyber Readiness Inspections (CCRIs), and provided support during and after CCRIs. Researched and interpreted Security Technical Implementation Guides (STIGs), providing clarity for customers. Scheduled and coordinated DISA-sponsored training as well as vendor training for USSOCOM. Planned and coordinated DISA Day at the USSOCOM IA Conference.

Information Assurance Rep

Computer Sciences Corporation (Assignments) - August 2010 to June 2011

As the DISA IA Field Security Rep, the liaison responsibilities were to identify problems, determine accuracy and relevance of information, and to use sound judgment to generate and evaluate alternatives, and to make recommendations. Responsible to provide technical security expertise in planning, preparing and executing additions to the Defense Networks and the Connection Approval Office (CAO) Process. Member of the Defense IA/Security Accreditation Working Group (DSAWG), and Secretariat Support requirements for DOD Service and Agency Information Systems. The primary POC for all USCYBERCOM/DISA IA interaction issues to include CCRIs, SAVs, Training, and RFIs. Active in the Joint Cyber Training Standards and Certification Writing Group and Executive Committee. As a member of the back office support team to a shared NOC, participated in Joint Training Exercises with Combatant Commands.

Information Systems Security Manager / Deputy PM

Computer Sciences Corporation (Assignments) - April 2007 to July 2010

As the onsite ISSM/ Deputy PM, was responsible for managing a government Information Assurance Support program that provided Certification and Accreditation (C&A) services for government information systems. Managed the support for seven subcontracting companies that supplemented CSC personnel on the C&A task, for a total of 60 plus contractors. Responsible for hiring CSC employees and approved subcontractor staff. Ensured optimum contract performance by convincing the government to upgrade and/or increase on-site positions. Performed other project management analyses as required.

Originally assigned to the Information Assurance Section (IAS) as a contract Information Systems Security Manager (ISSM) to one of the Department's high priority systems. Retiring two subsystems and successfully coordinating certification testing of another. Co-chaired the weekly Security Working Group at the program site and briefed Program status at the weekly IAS Unit Chiefs' meetings. Assisted in ensuring information technology (IT) systems and networks were in compliance with Federal governing directives for C&A, to include Privacy Impact Assessments (PIA) to identify and mitigate privacy risks. Prepared systems for FISMA Compliance Audits by reviewing system certification documentation for completeness and accuracy, to include the System Security Plan (SSP). Performed analyses and evaluated the suitability of proposed security architectures and security controls for new IT systems and networks. Independently developed Security Requirements Traceability Matrix (SRTM), validating the Plan of Action & Milestones (POAM) items providing identification of non-compliance of security requirements, and provided possible mitigation to requirements that were not in compliance. Maintained project information in the bureau's database and drafted electronic communications for approval to test (ATT) and approval to operate (ATO) in preparing the C&A Package. Also responsible for coordinating all activities between the customer and the C&A authorities for the process, helping to design new policies, standards, and methods where warranted. Active member of the Unclassified Network Internal Information Control Board, the Technical Change Control Board, and the Engineering Review Board advising other IT experts throughout the organization of issues, problems, or policies that may impact their IT solution recommendation. Or, complement another program for that matter.

Information Assurance Engineer

Braxton-Grant Technologies - October 2005 to April 2007

supported a government agency contract as a Systems Design Security Officer (SDSO) in the Information Systems Security Engineering Department. Assigned to telephony and distributed computing projects for new system starts and major system upgrades triggering re-accreditation. Liaison between the customer and C&A authorities for the process.

Designed the security architecture and ensured that the design and/or upgrades and enhancements were implemented with the appropriate security features and safeguards as outlined in DCID 6/3. Analyzed design specifications, design documentation, configuration practices and procedures, evaluated security controls, providing identification of non-compliance of security requirements, and provided possible mitigation to requirements that were not in compliance.

Developed Security Concept of Operations (SecCONOPS) and Systems Requirements Traceability Matrix (SRTM); developed and maintained client-approved best practices, processes, tools and approaches for the activities included with the client C&A process. Ensured the SSP reflected the current security posture of the system.

Security Systems Engineer

The Van Dyke Technology Group - November 2003 to October 2005

supported a government agency program which consisted of a team of Enterprise Audit System (EAS) Team members and stakeholders. The EAS Team was assigned to oversee the deployment of corporate enterprise audit solution-based on DCID 6/3 auditing categories (1-9) requirements. Defining, identifying, targeting, collecting, and processing of security relevant events. The centralized services also provided a robust solution to support Certification and Accreditation (C&A) requirements.
Served as the Development Manager providing oversight support for centralized vulnerability assessment. This task involved myriad Project Management activities to deliver on-time and within scope and budget. Presenting status, issues, and risk to upper management; taking into account the audience and nature of the informant, listening to concerns, and attending to nonverbal cues to respond appropriately. Prototyped and delivered several products such as the centralized Site Protector/Internet Scanner Vulnerability Assessment System. As well as worked with the DAA Representative to draft and implement the agency's C&A roadmap, to include methods, policies, and standards.

EDUCATION

Ph.D. in Information Technology

Capella University
March 2013

M.S. in Network Security

Capitol College
May 2005

B.S. in Computer Info Science

University of Maryland, University College
May 2002

SKILLS

Teaching (3 years), It Project Management (10+ years), IT Systems Security (10+ years)

CERTIFICATIONS/LICENSES

CISSP

PMP

GROUPS

ISC2

PMI

CFCP