# Mike Manoj

6412 Shannon Court, Clarksville, Maryland21029

**301-633-0776, Email: Mike.Manoj@Gmail.com**

###### E-SECURITY/E-GOVERNMENT SPECIALIST / IT SECURITY/PRIVACY/IT AUDIT

Creating and Driving Secure Digital Service Strategies for the New Economy

Reviewing the IT security measures and safeguarding the information resources of the enterprise to maintain integrity, confidentiality and availability of data / application, Risk Assessment & Risk Treatment

* Assessing IT requirements of the organization in terms of software, hardware and other peripherals / products, and handling procurement of the same
* Leading programs at customer site resulting in achieving high customer satisfaction and defining governance structure, best practices for project support and documentation
* Reviewing the physical & logical security measures and safeguarding the information resources of the enterprise to maintain integrity, confidentiality & availability of data
* Developing security operations procedure for efficient operation and protection of asset and property set up and maintain security integrity and function with strict rules and regulations
* Managing overall operations for executing projects involving scoping, initiating, high level design & architecture, resource mobilization, execution within cost & time parameters

**RELEVANT EXPERIENCE:**

* **Several advanced degrees**
  + M.S. Masters in Information Systems, 1992, Eastern Michigan University, GPA 3.6/4.0
  + **Graduate Merit Scholarship while pursuing Masters in Information Systems at Eastern Michigan University**
  + M.B.A. Master of Business Administration, 1988, West Virginia University, GPA 3.5/4.0
  + **100% Tuition covered Graduate-Assistantship while pursuing MBA at West Virginia**
* **More than 15 years of direct, IT, Security and Privacy experience**
  + Project Lead for “KPMG” information-technology audit, for the Prince Georges County Government, Office of Information and Technology
  + Overall 18 years’ experience in the information security field
  + Overall 22 years’ experience as a network-engineer, programmer, analyst, lead and manager
  + Worked extensively with several risk management tools such as RSA ARCHER, CSAM, RMS and EXACTA
* **Proven knowledge of FISMA, FedRAMP, Cloud Computing, Information Assurance, IT Audit, Privacy and security processes, tools and methodologies**
  + Supported solution development with subject matter experts and engineers to build the Cloud Solution Offerings and participates as a Solution Lead for Cloud Proposals and Opportunities.
  + Hands on experience with cloud service provider products and strong understanding of capabilities and limitations
  + Thorough understanding of Cloud Computing: virtualization technologies, Infrastructure as a Service, Platform as a Service and Software as a Service Cloud delivery models and the current competitive landscape.
  + Thorough understanding of infrastructure (firewalls, load balancers, hypervisor, storage, monitoring, security etc) and have experience with orchestration to develop a cloud solution
  + Thorough understanding of and/or ability to solution service offerings across all four tiers:   
    o Infrastructure (including outsourcing best practices, transition, and ITIL)
  + Application Development and Maintenance (including a basic understanding of various programming languages, SOA, and CGI’s development centers)
  + Thorough understanding of Government procurement policies and practices
  + Ability to strategize and develop complex responses to Government solicitations
  + Developed and performed security compliance in line with Cloud Computing FEDRAMP, FISMA, HIPAA, SARBANES-OXLEY,NSA,ISO 270001, Federal, State, and County- information technology regulations.
  + Conducted Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)
  + Formulated and enforced information security policies and processes for mission-critical information systems
  + Development of comprehensive risk assessment processes
  + Performed numerous risk assessments and IT audits ( in accordance with FEDRAMP, FISMA, NSA,ISO 270001, FISCAM, NIST 800-X Publications including NIST 800-53/A, CSEAT assessment, Federal, State, and County- IT infrastructure System
* Proven ability to work with clients, business partners and suppliers  
  + Supported numerous clients as a senior consultant
  + Successfully participated in management consulting, subcontracting and subcontract monitoring roles
  + Negotiated Supplier contracts
* Hands-on interfacing with the FISMA, FEDRAMP (Cloud Computing)/ NIST Risk Management Framework (C&A-FISMA/OMB/NIST)Process working with –
* Cloud-Computing FEDRAMP FAA NextGen/SWIM architecture initiatives
* Provides strategic focus, leadership, and presides over client engagements to elicit, document, analyze and validate IT security compliance by applying the latest Security Frameworks such as: Federal Risk and Authorization Management Program (FedRAMP), Federal Information Security Management Act (FISMA), NIST 800-53, Department of Defense Enterprise Cloud Service Broker (ECSB) and Risk Management Framework (RMF).
* Extensive experience in conducting Privacy Impact Assessments (PIAs), writing/performing security categorizations, Risk Assessments (RAs), System Security Plans (SSPs), Security Control Assessments (SCAs)/Security Test and Evaluations (ST&Es), Security Assessment Reports (SARs), Incident Response Plans (IRPs), Configuration Management Plans (CMPs), Information Technology Contingency Plans (ITCPs), and Plans of Action and Milestones (POA&Ms).
* Enterprise-wide Information Assurance Consulting assignments with multiple agencies such as National Oceanic and Atmospheric Administration (NOAA), **National Weather Service** (NWS), **Veterans Affairs** (VA), S**mall Business Administration** (SBA),and **Federal Aviation Administration** (FAA)
* Enterprise-wide review and preparation of Privacy Threshold Analysis/PrivacyImpact Assessment (PTA/PIA)
* Ongoing updated analysis of NIACAP/NIST Guidelines
* Automated Risk-Assessment using TS2000 software product
* HARRIS STAT tools vulnerability scan report
* Reviewed and prepared specific plans with NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.
* Reviewed and prepared specific plans with NIST SP 800-53Recommended Security Controls for Federal Information Systems and Organizations
* Reviewed and prepared specific plans with NIST SP 800-18- Guide for Developing Security Plans for Information Technology Systems.   
  Reviewed and prepared specific plans with NIST SP 800-30- Risk Management Guide for Information Technology Systems.
* Reviewed and prepared specific plans with NIST 800-34-Contingency Planning Guide for Information Technology Systems.
* **Numerous current professional certifications**
  + **CCSP** – Certified Cloud Security Professional – January 2016
  + **CCSK** – Certificate of Cloud Security Knowledge – June 2012
  + **CSSLP**- Certified Secure Software Lifecycle Professional– April 2009
  + **PMP**- Certified Project Management Professional – November 2007
  + **ISSMP** – Information Systems Security Management Professional – July 2004
  + CISM – Certified Information Security Manager , July 2003
  + CISSP – Certified Information System Security Professional , September 2002
  + Microsoft Certified Systems Engineer, **MCSE**, March 1999
  + Microsoft Certified Professional + Internet Certification, March 1999
  + Microsoft Certified Professional, March 1999
  + Certified Banyan Specialist, 1994, **CBS**, Ver 5.5
  + Certified Novell NetWare Administrator, 1995, **CNA**, 3.12
  + Certified NetWare Engineer, 1997, **CNE**, 3.12
  + Pursuing CIPP Privacy Specialist Certification
  + Pursuing HIPAA Security Specialist Certification

##### CAREER SKILLS/KNOWLEDGE

|  |  |
| --- | --- |
| * **Enterprise Management** | * **Security Management** |
| * Information Assurance * E-Commerce/Solutions Consulting * MIS/Systems Consulting * Proprietary Databases * Computer Telephony * Internet Audio/Video Technology * Client Relations/Development * Performance Management * Project Management * Configuration Management | * Homeland Security Initiatives * HIPAA Security initiatives and management * Authentication Software and Servers and Tokens * Biometrics * Access Control/Authorization, Single Sign-on, Web Access Control, Identity Management, Digital Rights Management * Assessment and Audit, Tools, Vulnerability Scanners, Penetration Testing,Forensics, Log Analysis Software * Security Policy Development, Configuration/Patch Management, Event/Alert Management, Perimeter Security * IDS, IPS,Wi-Fi Security, Email, Anti-Virus, VPN, Encryption |

###### CAREER ACHIEVEMENTS

* Developed Government/Corporate IT Security Program from the ground up. Developed Security Policies, Standards and Procedures. Created Corporate/Government Security Manual, System Security Guides and Compliance Checklists. Created corporate-wide auditing program and standards. Supervise and/or conduct periodic network security assessments and technical-engineering initiatives.
* Architect and deploy secure network infrastructures including Intrusion Detection Systems and Security Assessment Software.
* Plan and implement physical security controls for IT facilities. Manage long-term projects to improve security posture and capabilities. Develop and manage security awareness & training programs.
* Senior consultant managing large-scale, high profile strategy engagements for diverse clients in broad range of industries. Facilitate the formulation and execution of e-business strategies and plans, creating on-line businesses that meet clients’ unique needs in an increasingly competitive global marketplace.
* Providing senior information systems/information technology (IS/IT) executive experience to lead the client organization through a transition or to implement best practices and initial IT strategy and organization in a start-up.
* As the Network Analyst to Samba Insurance Company, worked on securing and re-designing the entire website with revamped contents and design architecture; Also, working on a strategic plan to integrate the IBM Mainframe with Windows NT network.

CAREER EXPERIENCE

FISMA/Cloud/FedRAMP/HIPAA Security Consultant

R2SEC LLC ([www.r2sec.com](http://www.r2sec.com)) October 2015 - Present

National Institute of Standards and Technology (NIST) August 2016 – Present

Evaluated cloud products such as Box, Office365, Skyhigh, Everbridge and related implication and gap analysis of controls implementation

Provided IT security risk assessment, management, and certification (C&A) services as a self-employed subcontractor for larger firms serving the U.S. Federal Aviation Administration (FAA); Deloitte Federal Services DC via LDAS, (a Federal cloud-based application), and smaller scale local projects.   
Assisted with hands-on with security planning, security compliance guidance under FISMA, OMB, and FedRAMP, as well as agency regulations, with risk assessment and planning services.   
Performed insightful business mission directed security risk assessments, control compliance and risk mitigation planning, vulnerability assessment and mitigation, contingency planning (CP) and incident response (IR) plan review, policy consulting and documentation.   
Advised clients in meeting relevant mobile device security controls, and security test criteria   
Provided outstanding Certifying Authority level services for several Federal agency systems, including review of many system procedures and policies for FISMA compliance, security scans, and FedRAMP compliance, covering all types of NIST 800-53 and Privacy Act controls.   
Developed and finalized application and network security control documents and supporting evidence, tracking tables, supporting valid data backup and transfer needs, defense-in-depth, mal-ware prevention, secure disposal of data and system assets. Shared security expertise in public outreach events.

Defense Health Agency, Falls Church, VA January 2016 – July 2016

[Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's IA posture](https://niccs.us-cert.gov/training/tc/framework/task-detail/397)

[Assure successful implementation and functionality of security requirements and appropriate IT policies and procedures that are consistent with the organization's mission and goals](https://niccs.us-cert.gov/training/tc/framework/task-detail/964)

[Collect and maintain data needed to meet system IA reporting](https://niccs.us-cert.gov/training/tc/framework/task-detail/440)

[Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)](https://niccs.us-cert.gov/training/tc/framework/task-detail/1041)

[Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.](https://niccs.us-cert.gov/training/tc/framework/task-detail/963)

[Ensure that IA inspections, tests, and reviews are coordinated for the network environment](https://niccs.us-cert.gov/training/tc/framework/task-detail/584)

[Ensure that IA requirements are integrated into the continuity planning for that system and/or organization(s)](https://niccs.us-cert.gov/training/tc/framework/task-detail/585)

[Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level IA architecture](https://niccs.us-cert.gov/training/tc/framework/task-detail/590)

[Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed](https://niccs.us-cert.gov/training/tc/framework/task-detail/598)

[Evaluate cost benefit, economic, and risk analysis in decision making process](https://niccs.us-cert.gov/training/tc/framework/task-detail/600)

[Identify security requirements specific to an IT system in all phases of the System Life Cycle](https://niccs.us-cert.gov/training/tc/framework/task-detail/962)

[Participate in an information security risk assessment during the Security Assessment and Authorization process](https://niccs.us-cert.gov/training/tc/framework/task-detail/731)

[Participate in the acquisition process as necessary, following appropriate supply chain risk management practices](https://niccs.us-cert.gov/training/tc/framework/task-detail/1017)

[Participate in the development or modification of the computer environment IA security program plans and requirements](https://niccs.us-cert.gov/training/tc/framework/task-detail/733)

[Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations](https://niccs.us-cert.gov/training/tc/framework/task-detail/790)

[Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents](https://niccs.us-cert.gov/training/tc/framework/task-detail/816)

[Recognize a possible security violation and take appropriate action to report the incident, as required](https://niccs.us-cert.gov/training/tc/framework/task-detail/824)

[Recommend resource allocations required to securely operate and maintain an organization](https://niccs.us-cert.gov/training/tc/framework/task-detail/828)

[Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered](https://niccs.us-cert.gov/training/tc/framework/task-detail/852)

[Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs, etc.)](https://niccs.us-cert.gov/training/tc/framework/task-detail/1016)

[Use federal and organization-specific published documents to manage operations of their computing environment system(s)](https://niccs.us-cert.gov/training/tc/framework/task-detail/869)

Department of Health and Human Services / CMMi

Centers for Medicare & Medicaid Services (CMS)

Center for Medicare & Medicaid Innovation (CMMI)

Business Service Group (BSG)

Woodlawn, Maryland October 2015 – December 2015

Provides subject matter expertise/ acts as a virtual ISSO. and consultancy to the Chief Information Security Officer in the areas of compliance governance and regulatory requirements. Determines the impact of new technology or policy (e.g., social networking, cloud computing, virtual environments, etc.) on the agency's information security program. Develops and implements information security program strategic and tactical goals and objectives. Develops and implement information security program outreach and communication plans. Identifies and develop a Performance Management program that includes performance measures, tracking metrics, and trend analysis. ​

Some other related responsibilities include:

* Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management)
* Assist in the determination of an appropriate level of security commensurate with the impact level
* Assist in the development and maintenance of system security plans and contingency plans for all systems under their responsibility.
* Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.
* Participate in self-assessment of system safeguards and program elements and in certification and accreditation of the system;
* Notify the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary;
* Maintain cooperative relationship with business partners or other interconnected systems.​

FISMA/Cloud/Fed RAMP Security Consultant, Department of Transportation (FAA), Office of ATO (FAA), Washington DC March 2006 – September 2015

* Cloud-Computing FISMA/FedRAMP/FAA NextGen/SWIM architecture initiatives
* Serve as a departmental expert for cyber security matters and is responsible for the coordination and integration of all aspects of the department's cyber, telecommunications, and information security programs.
* Provide supervisory leadership and direction to assigned subordinate staff within the Division of Cyber security and also assign, coordinate, and monitor the work of assigned contractor staff;
* Serve as Senior Technical Expert/Advisor to our senior IT management on all matters related to IT security and to our federal clients including information security policies, standards, directives, and guidance.
* Serves as a departmental/organizational expert for cyber security matters and is responsible for the coordination and integration of all aspects of the department's cyber, telecommunications, and information security programs.
* Responsible to answer to cyber threats and security incidents.
* Closely interfaced with multiple layers of management on program, policy, and process implementation
* Network and Security architecture, design, and implementation for government and commercial clients.
* Provided assurance-reviews of emerging security technology such as in Cloud-computing, and virtualization.
* Member of Audit and Compliance team, assigned to perform information system security audits of FAA information systems and Industrial Control Systems (ICSs).

Enterprise Security Consultant, Department of Veterans Affairs June 2005 – March 2006

Office of Web Ops, Veterans Affairs, Silver Spring, Maryland

* Worked as the enterprise security lead for the ongoing C&A process
* Participated in review of enterprise-architecture architecture
* Managed day to day operational trouble-shooting of the WebOps network security issues
* Provided reviews of emerging technology and products as expert analytical papers for decisions by executive management
* Closely worked with Management of Security Program Implementation
* Provided reviews of emerging technology and prepared expert analytical papers for decisions by executive management
* Closely worked with Management of Security Program Implementation

Information Security Analyst, Department of Commerce Dec 2003 – June 2005

Office of CIO, National Weather Service’s/Department of Commerce, Silver Spring, Maryland

* Worked as the security lead for the HOMELAND SECURITY initiative of delivering NATIONAL ALL HAZARD WARNING DISSEMINATION NETWORK through NOAA.
* Security leadership in C&A process
* Participated in review of enterprise-architecture shift into a full-mesh MPLS architecture
* Managed day to day operational trouble-shooting of the NCEP, NWS network security issues
* Provided reviews of emerging technology and products as expert analytical papers for decisions by executive management
* Closely worked with Management of Security Program Implementation

**E-Security/ IT Audit/ E-Government Coordinator** **July 2001– November 2003**

**Prince George’s Government County Office of Technology, Maryland**

**Architecture:**DMZ, VPN/ PIX FIREWALL 520, Cisco Switch - 2800, 2900, 3500, 4000, 5500, 6500,Cisco Routers - 2500, 2600, 7500; Hubs - Linksys, 3Comm,NetGear;WINDOWS 2K/NT Servers/Workstations, Unix, and Mainframe OS 390- multi-tiered environment; Bindview, Enterprise McCafee E-orchestrator Virus Protection; Cisco IDS/HDS integration with Policy Management tools; Bind-view security control with BV for Windows,SanctumAppShield, Appscan, Appaudit.

Headed up the security program management for the Office of Information and Technology, Prince George’s County. Major accomplishments include, among others, the following:

* Laying down the framework for a Security Management Program for the Agency in accordance with FEDERAL,STATE AND COUNTY Security Laws and Regulations
* Rolling-outPOLICYOPERATIONSCENTER product of BINDVIEW to initiate and implement program-management facets that include:
  + Creation of Security Program Charter
  + Creation of High-level program policies and best-practices
  + Creation of program procedures
  + Creation of technical standards and guidelines
  + Management, systems-admin and end-user awareness program
* Implemented programs and practices for IT AUDITING/SECURITY frame-work
* Constantly monitoring and improving compliance levels with FEDERAL, STATE AND COUNTY regulatory guidelines
* Coordinated **Homeland Security- TAMS System implementation/ HIPAA**-implementation project initiatives
* Key project lead for the e-government initiatives by the Prince George’s County office of technology
* Responsible for directing project teams of various agencies towards set project objectives.
* Manage and assist in the selection of outside Security and Disaster Recovery consultants.
* Research and management of e-government goals and implementation time-line.
* Worked with major vendors and solution providers and guided goals set by the agencies for e-government system implementation.

**CEO, Net Effort Inc March 2000- June 2001**

##### Net Effort.com, Maryland

* Oversee the security and privacy of corporate electronic information. Reviewed and selected new technology to support privacy requirements. Developed IT Privacy Policy and Web Privacy Policy.
* Planned and implemented growth for this company as an e-solutions/secure-services provider.
* Directed sales, marketing and operations to develop the business strategy to quarter-million revenue model within a year.
* Supervised engineering of all project implementations coordinating analysis, planning and implementation.
* Worked with major B2C, and B2B players in the market providing robust software application engines.

**Network Analyst August 1998 –Feb 2000**

##### Samba Insurance Company, Maryland

* Provided Information Security (INFOSEC) Support
* Provided Computer security support for Novell, Unix, and Windows NT LAN.
* Provided guidance for the development of HQ Network Firewall Systems.
* Planned and implemented complete Windows NT network layout, involving launching of Windows98 client workstations in a NT4.0 environment including management of resource planning and control.
* Directed the entire help desk trouble-shooting tasks of the windows NT/98/ IBM Mainframe network.

**Manager, Information and Communication Systems** **April 1996 - July 1998**

### **National Certification Commission for Acupuncture and Oriental Medicine, Washington, DC**

* Perform duties as Corporate Continuity Coordinator and Technology Risk Manager. Developed, implemented, and maintained the Business Continuity Program.
* Directed from start to finish, full-fledged implementation of the Website, nccaom.org, for the Organization, coordinating planning, development and implementation.
* Designed and implemented phone system with different vendors such as Lucent, Toshiba and Executone with hardware and software voice-mail system programming.

**Network Analyst**  **Jan 1995 – March 1996**

#### **BellAtlantic, Maryland**

* Provided senior level IT project management for software, and hardware deliverables
* Planned and integrated schedule, resources, and deliverables with IT departments and vendors
* Monitored project progress, and distribute reports to management and client, Develop Project plans, requirements documents, test plans & test cases, implementation plans, for elevating business software applications into a development, test, and production environments
* Communicated with internal client, team members, management, and IT
* Coordinated Technical Operation staff and QA

**Network Support Specialist** **July 1992 – Dec 1994**

### **Resolution Trust Corporation, Washington, DC**

* Developed and supported global corporate wide information security program.
* Research, develop and maintain Corporate Information Security Policy & Standards (for access control, encryption, workstation security, network security, etc.).
* Created Corporate Information Security Manual, System Security Guides, and Compliance Checklists. Promote InfoSec awareness by delivering training and education on security as required. Conducted Risk Assessments on Mainframe, Windows NT, Novell and Unix computer systems.
* Assisted users with maintenance of financial applications and design and production of reports resulting in an average savings of 50%.
* Trained users on financial software applications raising productivity by 40%.
* Advised key management personnel on areas such as end of year reporting, asset management, and legal reporting to help increase overall accuracy of financial reporting by the organization.
* Provided technical support of 600 server, 10,000 user nationwide Banyan Network.

**System Environments:**

|  |  |
| --- | --- |
| Security Management and Control Tools: | **CISCO Pix** Firewall- Policy Manager; **Bindview BV** for Windows Control Security Management; Bindview BV for Exchange Security Management for Exchange; **EPO- Orchestrator- McAfee** Virus Management Tool;  Hardware: **CISCO PIX 520**, Routers: 7500, 2600  Switches: 2900,6500; **Cisco AS5300** dial-up server; **TACACS+ Authentication** System; **CISCO-SECURE** Management Tool; **CISCO 4210 IDS** appliance. |
| Hardware | IBM ES9000, Compaq, HP, Macintosh, Gateways, CTI, Toshiba, Sony |
| Operating System | MS-DOS, Windows 3.x, Windows 95, 98, NT 4.0,TCP/IP, UNIX, VSE/VSA Release 2.3 |
| Case Tool | Structured Architect, Visible Analyst |
| Network | Internet, Banyan, Novell, Ethernet, TRing |
| Applications/Software | FrontPage 2000, Image Composer, CCMail, Microsoft Office 2000, Word 2000, Power Point 2000, Access 2000, Netscape, Eudora, Macromedia Dreamweaver, Internet Explorer, Dbase, Harvard Graphics, PhotoShop Adobe, Publisher 2000, Java, DHTML, XML. |

References available upon request