

RANDY M. NASH
nashr@atriskonline.com

OBJECTIVE:

I am seeking a challenging Information Systems Security position with a growth-oriented security-consulting firm where I can immediately apply more than 24 years knowledge, experience, and interpersonal/leadership skills, offering an opportunity for rapid advancement.

TECHNICAL SUMMARY:

I am an Information Security Consultant with high professional standards and a hunger for personal and professional growth. I will bring to your organization the confidence and professional attitude derived from over twenty years of technical experience. First certified in ADP Security and Risk Assessment in 1984, I have a long history of security experience not readily found in today's work force. I am widely experienced in Information Security, System Security, Network Security, Personnel Security and Physical Security. I have strengths in the areas of:

- Information Assurance (DITSCAP, NIACAP, NIST)
- Security risk and vulnerability assessments, evaluations, and audits
- Ethical Hacking and Penetration Testing
- Corporate Security Policy Development
- Application Security Testing
- Computer Forensics and Incident Response and Analysis

I have also written several articles on Information Security, and has been published at a variety of security web sites ([InformIT](#), [SecurityDocs](#), [HNS Security](#), and others).

EXPERTISE:

Network Operating System: Windows (all versions), Novell NetWare, and Unix (Linux, Solaris, *BSD).

Security Applications: Pedestal Security Expressions, Foundstone Scanner, Cisco HIDS, NAI Sniffer Pro, NAI CyberCop Scanner, NAI Gauntlet, NAI NetXRay, AntiSniff, ISS Security Scanner, ISS Database Scanner, ISS RealSecure, Retina, BlackICE Defender, PGP, Kane Security Analyst, SolarWinds Network Management Tools, Ethereal, Nessus, ngrep, dsniiff, ngrep, tcpdump/windump, snort/mysql/acid implementation, netcat, nmap, and various other port and vulnerability scanners. Also experienced with Wireless security issues.

Security Background: I have performed Certification & Accreditation (C&A), Security Testing & Evaluation (ST&E), and have developed full System Security Authorization Agreement (SSAA) documentation. I am experienced with DITSCAP, NIACAP, and NIST methodologies, procedures and documentation. I have performed security risk/vulnerability assessments, evaluations and audits, ethical hacking and penetration testing, corporate security policy development, application security assessments and audits, computer forensics, and incident response and analysis.

Security Clearance:

Previously held Top Secret, DoD, (inactive, 1992), and Secret (inactive, 2002).
Hold current NACI (DOJ)

CERTIFICATIONS:

- Certified Information System Security Professional (CISSP) – 2005.
- Cisco Secure IDS certification – 2001.
- INFOSEC Assessment Methodology (NSA Certification) – 1999.
- ADP Security and Risk Assessment certification – 1984.
- Preparing for CCNA and ISSEP.

RANDY M. NASH

EXPERIENCE:

BAE Systems (formerly DigitalNet)
Washington, DC

Jun 2004 – Present

Principal Secure Systems Engineer:

I provide consulting services for the Information Assurance practice, supporting clients in both the commercial and government sectors. His responsibilities include direct delivery of professional services, and development of strategic alliances with the security industry. Mr. Nash also:

- Develop Certification and Accreditation (C&A) packages for the office automation environments of various Department of Justice (DOJ) divisions. Provide security engineering expertise to the design teams, guiding the development of technical security controls.
- Perform vulnerability assessments based on the NIST SP 800-26 methodology, including development and execution of automated testing procedures,
- Develop system security plans and contingency plans based on the NIST 800 series,
- Provide network analysis and architectural guidance to identify methods for security risk reduction.
- Perform business impact analysis and risk assessments identifying critical risk areas, and
- Develop technical specifications and procedures for securing a variety of application platforms.

Avalon Technology
Arlington, VA

Nov 2002 – Jun 2004

Principal Consultant, Government Security Services:

Provided Business Development support, identifying and establishing strategic partnerships with many commercial and government entities. Developed an educational seminar for Certification and Accreditation (C&A) to be delivered via George Washington University as part of an effort to win new business and build name recognition for Avalon. Led the development of in-house tools to enhance government security offerings, and assist in the timely production of consistent customer deliverables.

At the FDIC, developed full C&A documentation in accordance with NIACAP and NIST guidelines for two Telecom General Support Systems (GSS):

- Developed complete System Security Authorization Agreement (SSAA) for two systems, with full supporting documentation package.
- Developed complete Security Plan and Risk Assessment documentation as part of the C&A process for FDIC Telecom.
- Developed and enhanced security policies and procedures in accordance with appropriate government guidelines.
- Developed ST&E Plan, and executed all tests. Completed ST&E Report, documenting findings from the ST&E process and providing recommendations to remediate identified weaknesses.
- Prepared formal response documents for GAO, IG and ISR findings. Developed appropriate countermeasures and implementation plans in response to these findings.

TMSI/FuGEN
Washington, DC

Feb 2002 – Nov 2002

Senior Security Analyst:

At the Dept of Treasury, developed C&A documentation in accordance with NIACAP for Treasury's HR Connect System:

- Performed Security Testing & Evaluation (ST&E) of HR Connect systems and environment.
- Developed Security Plan and Risk Assessment for pending C&A of additional sites.
- Developed and delivered Interim Authority To Operate
- Prepared documentation for System Security Authorization Agreement (SSAA).
- Developed security policies and procedures in accordance with appropriate government guidelines.

Predictive Systems, Inc
Herndon, Virginia

June 2001 – Feb 2002

RANDY M. NASH

Principal Security Consultant:

Provided senior level security consulting services to a variety of customers for Predictive Systems. These services included:

- Performed comprehensive Security Assessments for a variety of clients.
- Developed security policies and procedures.
- Assisted Predictive's SOC with incident response, analysis and cross-correlation of events.
- Provided Customer Relationship management for a key government client.

Provided critical Business Development support, establishing a partnership with a company focusing in Physical Security and Counter-Terrorism to focus on National Critical Infrastructure clients. Responsible for \$.5 million in sales in Q4, 2000, and had approximately \$1.5 million in the pipeline at the time of his departure.

BlueStorm

February 2001 – June 2001

McLean, Virginia

Senior Security Consultant:

Provided senior level security services and Business Development support for BlueStorm. Mr. Nash participated in business development strategy meetings and assisted in the development of security business offerings and methodologies for security engagements as part of the business development efforts at BlueStorm and:

- Researched and assisted in the development of new business offerings in the areas of HIPAA compliance and Computer Forensics, and Incident Response and Analysis.
- Assisted in writing business proposals and Statement's of Work (SOWs).
- Performed Vulnerability and Risk Assessments for various BlueStorm clients.

Predictive Systems, Inc

June 2000 – February 2001

Herndon, Virginia

Senior Security Consultant:

Provided senior level security consulting services to a variety of customers for Predictive Systems. These services included:

- Performed comprehensive Security Assessments for a variety of clients.
- Developed security policies and procedures.
- Participated in multi-practice Gap Analysis for various customers. Performed Application Security assessments of online banking solutions.
- Developed in-house procedures and documentation to enhance Predictive's business offerings.

STG, Inc

July 1999 – June 2000

Fairfax, Virginia

Senior Security Analyst:

Provided senior level security consulting services for the Dept of State in the following capacity:

- Assisted with Incident Response and Analysis when a State Dept web server was compromised.
- Served as Technical advisor and voting member of State Department's PKI Technical and Business Working Groups. Non-voting member in Federal PKI Technical and Business Working Groups.
- Performed Security Testing and Evaluation (ST&E) for various State Dept bureaus in accordance with DITSCAP methodology and procedures.
- Researched and evaluated the latest technology in the security arena (i.e., VPN's/IPSec, PKI, X.509, encryption, FIPS validations) for possible implementation.
- Developed IIS Secure Configuration guidelines and policies.

Seneca Support Technologies

March 1995 – July 1999

Vienna, Virginia

Director, Intel Support Services:

I worked for Seneca Support Technologies for over 4 years, and served in a series of positions of ever-increasing responsibility, culminating in his position as Director of Intel Support Services.

RANDY M. NASH

- Performed in-house security assessment of critical information systems. Developed and implemented roadmap for improved security posture.
- Maintained a hardened database server based on Windows NT. Tracked and managed patch level to address new vulnerabilities as they were discovered.
- Manage a technical staff of 12-15 consultants providing Mac and PC support. Provide technical evaluation of all incoming consultants based on client needs.
- Installed and configured Seneca's first Internet router/server/firewall utilizing Linux. Hosted http server, caching proxy, POP/SMTP email and PPP access via this same system. Additional security was managed via IP filtering and TCP wrapper.

Senior Systems Security Engineer:

- Provided incident response, analysis and auditing capabilities.
- Implemented C2 Security specifications in Windows NT 4.0 enterprise network.
- Evaluated Security Auditing Tools for Windows NT enterprise network.
- Provided liaison with Microsoft Corporation for testing and evaluation of beta-release products (i.e., Windows 95/98, Windows NT/2000, Office 2000, etc.).
- Assisted in the development of a client-wide plan for proper computer virus control.

Metters Industries, Inc Arlington, Virginia

December 1993 - March 1995

Network Engineer: As a Network Engineer, developed, configured, and maintained an Enterprise Network backup solution encompassing 20+ Novell file servers with approximately 22GB of information. Developed and implemented new software and hardware configurations to support the SPAWAR Wide Area Network (WAN). Assisted in various network management tasks such as Domain Name Services (DNS) maintenance, and assignment of IP addresses. Provided security assessments of existing architecture and product implementations (Novell 3.11, Remote Access, and Internet Access). Assisted in the building of a Linux-based web server to replace one compromised (trojaned, back-doored) by previous administrator.

U.S. Army Materiel Command (MWR) Alexandria, Virginia

June 1992 - December 1993

Computer Specialist: Maintained 100-user, single-server Novell Local Area Network (LAN) running DOS and Windows applications. Performed Oracle Database Administrator (DBA) tasks for the Beta-test of a Financial Management Application, and conducted formal and informal seminars and training sessions to exchange automation concepts, ideas and techniques. Developed and maintained training guides and submitted quarterly articles on automation topics.

- Developed network security administration standards and guidelines for all MWR activities.
- Implemented User Security Awareness training in the form of presentations, bulletins, and articles.

United States Marine Corps

September 1980 - June 1992

Mainframe Security Administrator: Performed mainframe security administration for Marine Corps-wide network. Managed access controls for approximately 1400 geographically dispersed users. At this time (1984) I received my certification in ADP Security and Risk Assessment and performed Security Risk Assessments for various data processing activities.

Computer Programmer: Trained in mainframe COBOL, EDL (Event-Driven Language), Clipper and Ada. Served as lead analyst/programmer on the Marine Corps Marathon Race Scoring System.

REFERENCES:

Available upon request.