Eric D. Williams
Expert IT Security/Administration Consultant

E-Mail: eric@infobro.com
1309 "S" Street S.E.
Washington DC 20020-6925
+1.202.889.4395 Voice / +1.202.889.4396 Fax

Professional Experience

- Currently: Expert Security Consultant on Internet and Computer Security for National Oceanic and Atmospheric Administration
- Past Roles: Expert Security Consultant: Design, Policy Development, Testing and Implementation of internetwork security for: Bureau of the Census, NOAA, Department of Commerce
- System Administration and Security Consultant for several area ISPs
- Numerous Security Consultation efforts under non-disclosure for "major media" outlets.
- Numerous Security Consultation efforts for Government Agencies.
- Over 12 years professional experience in Computer and Computer Communications Technology
- Recognized industry expert in implementation of OSI and Internet Protocol Suite technology.
- Experienced in advanced technical writing, presentation, and marketing.
- Senior Systems and Internetwork Engineer with experience in DoD and Private Industry
- Past Chairman - Convergence Working Group of the Open Systems Environment Implementors Workshop (OIW) OSETC (defunct), sponsored by the IEEE, Active Member of the Internet Society (ISOC) DC Chapter
- Participant in the Internet Engineering Task Force working groups on IP next generation (IPng), Internet Mail Extensions (mail-ext), Electronic Data Interchange integration (EDI-INT), Intrusion Detection (idwg), Public Key Infrastructure (pkix), Responsible Uses of the Internet (RUN) and others
- Contributor to numerous Internet security forums and discussion lists (eric@infobro.com)
- University of Maryland Baltimore County: 1983-1987, Biology / Music (NDC) - "my first love was always computers…"
- Member of the Information Assurance Task Force (www.iatf.net)
- Certificate of Completion National Security Agency - INFOSEC Assessment Methodology Course (July 2000)
- Clearances: Current Government SAC and NACI Background Investigations

President / Principal Consultant; Information Brokers, Inc. April 1995—Present

Mr. Williams is responsible for all management and program operations of this information and computer communications organization. Mr. Williams is a recognized industry leader in implementing open system solutions and Internet security. Mr. Williams consults leading market research firms and publications to advise on industry trends, Black Enterprise Top 100 companies, Fortune 500 companies and the Federal Government; for Internetwork design, and particularly expertise in the field of Internet Security, protocol design and implementation. Through numerous engagements Mr. Williams has transformed the understanding of IT security awareness and risks associated with inadequate IT security controls internationally. Mr. Williams is knowledgeable in numerous methods concerning the application of computer forensics and security used to detect and combat hacking and *Cyberterrorism*.

Technical Projects, Programming and Operating System Experience

National Oceanic and Atmospheric Administration (NOAA)
Reston Consulting Group (RCG) – May 1996—Present (Consultant)

Mr. Williams contracts with Reston Consulting Group to develop policies, guidelines and implementation parameters for the NOAA Telecommunications and ADP Security Branch (now known as the Information Technology Security Office.) Here are some of the effects of Mr. Williams' activities in the following areas, NOAA-wide:

Information Brokers, Inc.   Phone: +1 (202) 889-4395
1309 'S' Street S.E.   Fax: +1 (301) 889-4396
Washington, DC 20020-6925   V-Mail: +1 (301) 303-8998

http://www.**InfoBro**.com/   info@**InfoBro**.com

- Secure Infrastructure Implementation and Policy – Enabled NOAA to establish system inventory information and standards that allow efficient implementation of security in all types of systems.
- Computer System Security (Implementation and Policy) – For Major Application and General Support systems, enabled NOAA to disseminate and educate its constituencies with information about secure systems, improving the overall NOAA security posture.
- Information Security Policy – Work with NOAA on policies for IT security has in conjunction with training activities reduced the overall risk of IT security compromise.
- Security Awareness Training – Education through lectures, workshops and working groups improved the awareness throughout NOAA commensurate with risks to its systems and transformed the IT culture NOAA-wide, especially as related to IT security.
- Computer Security Incident Response – Developed security guidelines and policies that established the NOAA Computer Incident Response Team (N-CIRT) and enables NOAA to respond proactively to security vulnerabilities. During response to computer security incidents involving the NOAA infrastructure, Mr. Williams' unique approach enabled improvements in cooperation between the various NOAA line operating units and NOAA headquarters.
- Security Architecture development (NOAA-wide) – Facilitated understanding of the ten domains of successful IT security management, Mr. Williams' understanding and incorporation of government and industry best practices closed critical gaps in the baseline IT security implementation at NOAA.

Under the auspices of NOAA IT Security advisor, Mr. Williams' was the only contractor personnel to serve, as technical advisor, on the 2001 Department of Commerce IT Security Task Force and its working groups. The task force—formed to develop strategies and actions—addressed information security deficiencies identified by General Accounting Office auditors. Mr. Williams developed the governing language for "Action Alerts" that were distributed Department-wide. The alerts were essential to the Department for addressing immediate IT security concerns and closing 'holes' identified in the Department IT security infrastructure.

Incident Response and Reporting Policy –Occupational Health and Safety Administration (OSHA)
RCG – June 2002—Present (Consultant)

Development and analysis of Occupational Health and Safety Administration (OSHA) capabilities and policies concerning computer security incident response and reporting. This is the first and most comprehensive effort to address computer security incident response and reporting in the OSHA environment. The contract also included: Development of an OSHA-wide policy for incident response; training at the OSHA computer security seminar; system administrator's emergency action handbooks and tools; and high-level analysis of OSHA computer security capabilities allowing better understanding by OSHA management.

IT Security Policy Development – US Department of Commerce
Computers and Hi-Tech Management, Inc. (CHM) / RCG – Sept. 2001—Sept. 2002 (Sub-Contractor)

Mr. Williams served as key personnel on development of revisions of the Department of Commerce IT Security Program policies. The tasking involved the incorporation of best practices and industry standards for addressing IT security throughout the Department. The policy development revised the aging policies that were in place at the start of tasking. This policy has brought all Departmental operating units into alignment with new IT security program requirements developed by the Department of Commerce IT Security Task Force working groups.

Compliance Reviews of Operating Unit Security Programs – US Department of Commerce
CHM / RCG – September 2001—September 2002 (Sub-Contractor)

Mr. Williams participated in the development and implementation of the Department guidelines for security programs and metrics for compliance with the Department security policies and program.

Information Brokers, Inc.
1309 'S' Street S.E.
Washington, DC 20020-6925

Phone: +1 (202) 889-4395
Fax: +1 (301) 889-4396
V-Mail: +1 (301) 303-8998

http://www.**InfoBro**.com/   info@**InfoBro**.com

Work included advising working groups that developed the metrics for compliance review. Under Mr. Williams' leadership, review teams and metrics were prototyped for future review processes throughout the Department. The prototypical teams reviewed the Bureau of Census and Bureau of Economic Analysis. The review teams produced and standardized reports and recommendations for the Department and its operating units on compliance with Federal and Department past and current program requirements as well as industry standards for information technology security.

Risk Assessment and Risk Mitigation Strategy – US Department of Commerce
CHM / RCG – August 2001—April 2002 (Sub-Contractor)

Qualitative risk assessment and mitigation strategies for the Department of Commerce (DoC) Herbert C. Hoover Building (HCHB) integrated network. This activity identified cost effective methods for sharing essential infrastructure components. Additionally, work during this task documented the critical interrelationships between DoC operating unit system, allowing for the first time a comprehensive view of inherent IT security risks Department-wide. The results of the entire effort allowed the Department to address policy and technological concerns in a comprehensive manner through use of a methodology developed to apply the Common Criteria v2.1 and protection profiles for network component targets of evaluation. The DoC network implementation includes all Department headquarters and operating unit networks and information resources housed at the HCHB facilities and included assessment and development of policies to address remote access and mobile users. The risk mitigation strategies utilized methodologies of the Common Criteria to develop a robust technically secure environment during network deployment.

Risk Assessment – National Environmental Satellite Data Information Systems (NESDIS)
RCG – June 2000—August 2000 (Consultant)

Mr. Williams completed a comprehensive security risk assessment of the NOAA National Virtual Data System, a system used to provide all NOAA data center information in the public domain. The analysis was the pre-cursor and a primary element in facilitating security "tightening" for this popular and crucial NOAA information dissemination resource prior to its public roll-out by NOAA. This analysis was essential for identifying requirements of contractors for future e-commerce projects and NOAA standards for implementing distributed e-commerce systems. The risk analysis included scanning for system vulnerabilities, source code analysis (of Oracle 8i Web and Database applications) and authorized security exploits utilizing social engineering tactics on government and private industry subjects.

Enterprise Architecture Training – United States Agency for International Development (USAID)
Computer Frontiers, Inc. – June 2000—November 2000; January 2001; May 2001 (Consultant)

Under the USAID Leland Initiative, in June through July 2000, Mr. Williams authored and conducted a 5-day workshop on the development of Information and Communications Technology (ICT) enterprise architectures for the Government of Uganda and Makerere University. These efforts have led to the establishment of coordinated ICT programs between the academia and government, and the establishment of new academic fellowships at the University. Subsequently, Mr. Williams returned to Uganda to follow-up on the establishment of a Makerere University ICT Architecture Task Force.

Mr. Williams also conducted meetings and advised Ugandan ISP's on the implementation of metropolitan internetwork exchange point implementation. This activity has led to the active cooperation of internet providers from Kenya, Uganda and others in the region for establishment of cost-effective continental and international internet connectivity.

In May of 2001, Mr. Williams traveled to Lesotho, also under the Leland Initiative, in South Africa to lecture and advise the Lesotho Ministry of Telecommunications on the establishment of tariffs and architectures for telecommunications privatization. This effort established an Architecture working-

Information Brokers, Inc.   Phone: +1 (202) 889-4395
1309 'S' Street S.E.   Fax: +1 (301) 889-4396
Washington, DC 20020-6925   V-Mail: +1 (301) 303-8998

http://www.**InfoBro**.com/   info@**InfoBro**.com

group in the Ministry of Telecommunications that establishes standards for privatization plans and expectations of providers that are business and community friendly.

System/Security Administration and Network Support Engineering
Metters Industries, Inc./MettersMEDIA Network, Inc.; April 1996—Present (Consultant)

Mr. Williams and Information Brokers, Inc. provide engineering and technical support for system and network operations of Windows NT and Unix systems (Sun, SGI, Linux). This engagement allowed MettersMEDIA Network to win the contract for management of the HUD Housing Counseling Clearinghouse and USAID Leland Initiative country websites. Under this agreement an ISP operated by MettersMEDIA network was supported until the company closed business in 2002. During that time, Mr. Williams provided technical support for all aspects of Internet integration and operations including multi-homed and virtual hosting of websites, e-mail, ftp and domain name system support.

Firewall Test and Implementation Plan - US Dept of Commerce, Bureau of the Census -
American Technical Resources (ATR) / RCG – September 1995—April 1996 (Consultant)

Mr. Williams completed planning and implementation of the Bureau of Census' first internetwork firewall system. The work provided by Mr. Williams allowed the Bureau of Census to successfully implement new policies and security technologies for all Census systems. Mr. Williams presented lectures concerning policy and implementation considerations, designed and developed a test plan testing the integrity of the vendor implementation and conformance with requirements. The system consisted of an ANS Interlock Application Gateway Firewall and router filter security. MAC spoofing test results were crucial in the design and implementation of the secure system, and at the time represented the only known published ethernet switch MAC spoofing test suite.

Programming
C, C++, Ada, Prolog, BASIC, COBOL, FORTRAN, Pascal, HTML; UNIX shell scripting using csh, ksh, sh, bash, awk, sed, perl, CGI and many other macro languages and programming environments.

Security Tools
Cisco PIX Firewall, Checkpoint Firewall-1, ISS RealSecure, SNORT (freeware) IDS and protocol implementation and analysis, various host and network based intrusion detection and prevention technologies, e.g. tripwire, COPS, tcpdump, ethereal, etc.; network and host security scanner technologies, e.g. l0pth Crack, nmap, RETINA, SARA, SATAN, SAINT, netcat, etc.; computer security forensics tools, e.g. dd, lsof, ltrace, md5sum, strace, The Coroner's Toolkit (tct) [lazarus], truss, etc.

Operating System / Environment
DOS all versions, Windows all versions including Windows 2000/9x/NT/ME/XP, Bayan VINES, Novell Netware, SunOS, SunOS/Solaris, OpenWindows, SGI IRIX, BSD-386, Linux, SCO UNIX, OS/2, Coherent 4.x, DR-DOS, Concurrent DOS, Desqview, X Window, VMS, MVS, RTOS; Macintosh System 6-9, A/UX (Macintosh UNIX), HP/UX, AIX; Plan 9, Numerous OS platforms too numerous to list have been utilized.

Computer Communications Networking and Protocols
Ethernet; Wireless Ethernet; FDDI, Token Ring, ATM, ATM LAN Emulation, SONET, ISDN, SMDS, xDSL, Frame Relay, X.25, Protocols: SPX/IPX, XNS Protocols, Vines IP, NetBIOS/NetBEUI, Client/Server protocol design/implementation; IPS protocols: DNS, TCP, IP, UDP, ICMP, POP 1-3, IMAP 2-4, IRC, SMTP, NNTP, NTP, OSF DCE protocols, Sun RPC, HTTP, FTP, RFC1006 implementation, MIME, Mobile-IP, RIPSO, OSPF, RIP, IGRP, EGP, BGPv4, Telnet, Gopher, IP over ATM, SNMP; IPv6, Routing, Encryption protocols; X.400 (X.420 - EDI), X.500, FTAM, VT, CMIP, GNMP, router implementation including POTS network integration, Leased line implementation. Cisco, Bay Networks, Cabletron, Timeplex.

Reference contact information available upon request.
Personal URL: http://new.infobro.com/AboutUs/People/EricWilliams/ericwilliams.html

Information Brokers, Inc.
1309 'S' Street S.E.
Washington, DC 20020-6925

Phone: +1 (202) 889-4395
Fax: +1 (301) 889-4396
V-Mail: +1 (301) 303-8998

http://www.**InfoBro**.com/   info@**InfoBro**.com