PAUL E. WOODIE, JR., CISSP

305 Grindstone Drive
Arnold, MD 21012
Telephone: 443-924-0336
Email Address: paul.woodie@verizon.net

SUMMARY OF SKILLS:

Computer systems forensics, analysis, and configuration related to cyber security (Microsoft Windows and Linux systems). Teaching, briefing, coaching, and mentoring of others in computer and network systems security. Formal technical classroom instruction in computer networking and security technical areas in both academic (US Naval Academy, industrial (Defense Security Service -DSS-Academy), US Government [National Security Agency (NSA)] and professional settings (Learning Tree). Developed and presented lab-based training courses for both US Naval Academy, Learning Tree, and DSS. For example, I was the technical editor during the development of a lab-based Learning Tree course on Public Key Infrastructure (PKI) technology. I also taught both firewalls and internet security classes for Learning Tree. Resolution of technical implementation issues in the application of computer and network security standards in the classified DoD contractor community. Analysis of computer and networked information systems against established information security standards (at the National Computer Security Center). Leadership and/or participation in various standards and interagency panels and working groups.

EXPERIENCE:

March 2011 to present
Woodie Cybersecurity Associates

Developed and taught a two day course in Cybersecurity to US Government security professionals. This hands-on course includes cyber threats, laws, countermeasures, and tools to test a system's cybersecurity posture. As part of the class, a set of cybersecurity tools and resources are provided to the student and used in the class. This provides an opportunity, through hands-on exercises, to “learn by doing.” Taught NISPOM Chapter 8 standards and practices for getting a computer system “Certified and Accredited” to process classified information.

November 1999 to March 2011
DSS

Curriculum Manager, Information Assurance, DSS Academy

Develop and present training at the DSS Academy based on the computer security standards contained in the National Industrial Security Program Operating Manual (NISPOM). This training is lab-based, where students not only learn about computer and network security, but also apply in a lab environment the skills that they are learning by configuring both Linux and Windows XP Pro computers to comply with current cyber security standards. My role includes not only teaching, but also developing, maintaining, and troubleshooting the lab exercises which include security configuration, shell

programming, network sniffing and mapping, security diagnostics, and automated setup of security parameters. This is done in both Windows and Linux environments. Samples available if needed. Includes extensive work with security tools such as Helix, System Rescue CD, disk and file systems analysis, disk partitioning schemes, internal operating system auditing structures and other security parameters.

At the direction of the DSS/IG, conducted a computer systems forensic analysis as part of an internal computer systems investigation.

Speaker at numerous national conferences, including the DoD PKI conference in Las Vegas (use of PKI with Linux). Provided training in DSS to both systems administrators and users in the application of PKI in the DSS environment. Distribution and installation of DoD PKI certs to DSS employees and resolution of various client PKI problems. Helped Learning Tree develop their first course in PKI technology. Taught Basic Security and Firewalls courses for Learning Tree.

Actively participate in the National Industrial Security Program community in resolution of technical problems and issues associated with application of published security policies and standards in the classified DoD contractor community. For example, have contributed to standard approaches to Linux authentication and automated audit, including configuring commercial hardware and software systems to comply with published standards. Application of forensic techniques for identification and retrieval of data hidden in various storage media. Analysis of network traffic to determine information leakages and non-compliant information flows.

October 1998 to November 1999
DSS

Technical Director, Security, DSS

Provided technical direction (as Technical Director for security) to computer and network security personnel in DSS. Provided training and mentoring in computer and network security for those in DSS who are responsible for accrediting computers and networks in the DoD contractor community. Participated in many DSS-wide panels and evaluation teams focusing on application of national computer security standards applicable to the DoD contractor community. Initiated use of PKI at DSS.

July 1991 to October 1998
NSA

Assisted a wide variety of U.S. Government customers to identify their security needs and select the most appropriate security solutions to meet those needs. This covered a wide range of security technologies including trusted operating system technology, encryption technology, firewalls, high-assurance firewalls/guards, and network encryption protocols such as SSL, s/MIME and accompanying PKI.

July 1988 to July 1991
NSA

Conducted research in analog and digital communications related to digital signal processing

techniques. This included designing real-time hardware and software for Unix systems data acquisition.

December 1980 to July 1988
NSA

Evaluated numerous commercial computer systems (e.g., IBM, Digital Equipment Corp., etc.) to determine system security properties. The goal of these evaluations (a.k.a. Orange Book evaluations) was to determine suitability for use by the U.S. Government. Developed the evaluation process and staffed it to create a growing "Evaluated Products List." Developed, coordinated, and implemented interagency cryptographic protection standards for digitized voice and computer communications networks.

August 1964 to December 1980
Miscellaneous

Broad experience, both inside and outside of US Government, in communications- and computer engineering organizations with wide involvement in many aspects of those businesses including: requirements analysis; applications engineering; detailed engineering design; field and depot level diagnosis, maintenance, and training; customer engineering and analysis; technical writing; and marketing. This experience covers commercial, civil government, and military systems.

EDUCATION:

Bachelor of Engineering Science, Johns Hopkins University, 1964, (E.E.)
Master of Engineering Administration, George Washington University, 1980, (Mgmt)
Many specialized technical and management courses

PATENTS AND PUBLICATIONS:

1969, Patent on Digital Communications Systems Design

1983, "Security Enhancement through Product Evaluation," IEEE Computer Society Symposium on Security and Privacy

1983 "All I ever wanted to know about the Data Encryption Standard," IEEE Newsletter for the Technical Committee on Security and Privacy

1985 1986, Workshop leader at annual Computer Security Institute Conference on Computer Security

1986 "Distributed Processing Systems Security: Communications, Computer, or Both?", IEEE Conference on Data Engineering

1993 "Multilevel Information Systems Security," U.S. Department of Energy Computer Security Conference

1994 Multilevel Information Systems Security for Military Applications," Military Communications (MILCOM) Conference

1994 Panelist at the National Information Systems Security Conference, Baltimore, MD, Presentation on the "Multilevel Information Systems Security Initiative (MISSI) approach to network security

2000 Speaker at the DoD PKI Conference in Las Vegas. Topic: Use of DoD PKI in a Linux environment. Included a live demonstration.

2001-12

Speaker at the National Security Institute national conference. Topics related to computer security standards relevant to the DoD contractor community.