

James L. Henderson/CISSP
12119 Willow Wood Drive
Silver Spring, Maryland, 20904
E-Mail-cybercops911@comcast.net
Cell Phone-561-809-6800

CURRENT CLEARANCE LEVEL: TOP SECRET SCI W/DIA CI POLYGRAPH

SUMMARY OF EXPERIENCE / RESPONSIBILITIES

- **15 Years of Hands-On Experience:** In the development, implementation and management of complex Enterprise Information Systems Security Programs, Information Assurance Risk Management Programs and Insider Threat Risk Management Programs for the DoD, National Level Intelligence Centers, Federal Agencies and State Governments. My primary focus has been in the areas of Information Assurance Governance, Risk Management and Compliance.
- **Held Senior Level Enterprise Program Management Positions As:** Information Assurance-Cyber Security Training Instructor, Senior Information Assurance Manager/Engineer-Subject Matter Expert, Director Of Information Systems Security / Continuity Of Operations Program (COOP) Manager, Designated Approving Authority Representative / Certifier Of Information Systems, Computer Forensics Examiner/Analyst, Information Systems Security Manager (ISSM). Have provided strategic planning, operational direction, managed multiple teams, tasks and the financial resources for all projects under my direction, and have reported directly to Agency Directors and Senior Level Management.
- **Director Of Information Systems Security / Senior Information Assurance Manager-Engineer Responsibilities:** Protected the confidentiality, integrity and availability of mission critical classified information and information systems up to the Top Secret SCI Level. Apply defense-in-depth strategies using multiple layers of security; Physical / Operational Security, Counterintelligence, Network Perimeter, Application Layer, Storage Layer, Data Layer, End Points. Developed, implemented and managed Enterprise Top Secret SCI Information Assurance-Information Systems Security Programs for the DoD. **Major Responsibilities Have Included:** Defining the Information Systems Security Program Framework/Governance Structure, Security Policy and Security Classification Guide Development, Data Privacy Protection / Personally Identifiable Information (PII), Conducting Risk Assessments/Mitigation, Performing Certification/Accreditation of Information Systems for JWICS, SIPRNET, NIPRNET Networks, **Managing The;** Configuration Control Board, Security, Education, Training, Awareness Program, COOP/Disaster Recovery Program, Computer Security Incident Response Team.
- **Provide Information Systems Security Engineering Guidance In The Areas Of;** Emerging Cyber Attacks/Threats, Advanced Persistent Threats, Computer-Network Forensics Tools, Data Loss Prevention Tools, Insider Threat Auditing Tools, Security Technical Implementation Guides (STIGS) for Operating Systems-Applications, Vulnerability, Patch Management, Continuous Monitoring and SCAP Tools, Secure Software Coding Practices, etc.
- **Counterespionage / Information Systems Security Program Management Training Instructor:** Develop and currently teach a comprehensive Counterespionage-Insider Threat Defense Training Course and Information Systems Security Program Management Training Course / DNI ICD 503, to security professionals for the Federal Government and DoD/IC Agencies. **Proficient With The Following:** OMB Memos, FISMA, Privacy Act, SANS Consensus Audit Guidelines, U.S. Government Configuration Baseline (USGCB) / FDCC, DISA Security Technical Implementation Guides (STIG's), NIST/FIPS Special Publications, CNSS Instructions/Policies, DNI ICD 503, DCID 6/3, DCID 6/9, JAFAN 6/3, CJCSI 6510.01E-Information Assurance-Computer Network Defense, DIACAP/DoDI 8510.01, DoDI 8500.2 IA, DoDI 8502.03 PKI, DoD 5105.21-M-1 SCI Admin Manual, Joint DODIIS SCI Information Security Standards, NISPOM DoD 5220.22-M, DoD 5200.1-R Information Security Program, DoD 5240.06 Counterintelligence Awareness and Reporting, Health Insurance Portability & Accountability Act (HIPAA), PCI Data Security Standards, Cloud Security Alliance Cloud Controls Matrix.

CERTIFICATIONS / PROFESSIONAL MEMBERSHIPS AND RECOGNITION

- **Certified:** CISSP/Certified Information Systems Security Professional
- **Certified:** Computer Forensics Investigator By NTI
- **Certified:** Security Systems Engineer / Network Traffic Intrusion Analyst
- **Certified:** Network Security Professional (Advanced) By High Tech Crime Network
- **Certified:** CheckPoint Firewall Certified Systems Administrator
- **Certified:** Microsoft Certified Professional NT Server 4.0 / Microsoft Network Essentials
- **Recognition:** Information Assurance Subject Matter Expert-DoD Information Assurance Technology Analysis Center
- **Chairman:** FBI Infragard / Insider Threat Special Interest Group
- **Member:** Federal Information Systems Security Educators' Assoc. (Recipient 2010 Security Awareness Website Award)

SPECIALIZED TRAINING

- Designated Approving Authority / DAA Training Course – Taught By Defense Information Systems Agency (DISA)
- SCI ISSM Training Courses (Navy / Air Force), Army IA Information Assurance Fundamentals Training Course
- NSA InfoSec Assessment Methodology / Information Security Audits And Assessments -Taught By NSA
- EnCase Computer Forensics Investigator Training Course - Taught By DIA National Media Exploitation Center
- Raytheon InnerView-Insider Threat Focused Observation Tool Investigator Training – Taught By Raytheon
- Best Practices For Mitigating Insider Threats - CERT Insider Threat Center

References, Training-Certification Documentation Furnished Upon Request

James L. Henderson/CISSP
12119 Willow Wood Drive
Silver Spring, Maryland, 20904
E-Mail-cybercops911@comcast.net
Cell Phone-561-809-6800

PROFESSIONAL EXPERIENCE

Information Assurance / Counterespionage-Insider Threat Defense Training Instructor

October 2011 To Present

DoD Defense Security Services (DSS CDSE) - Linthicum, Maryland (Contractor: CACI)

- Assist in the design, development and instruction of DSS IA (NISPOM Chapter 8), Cyber Security and Counterespionage training courses, supporting the National Industrial Security Program (NISP) and Defense Industrial Base (DIB), using the ADDIE Instructional Design Model and NIST SP 800-50: Building an Information Technology Security Awareness and Training Program.
- Establish an Information Technology Security / Information Assurance (IA) Essential Body of Knowledge (EBK) that provides for a baseline framework of essential knowledge and skills that IT, IA, Security and Counterintelligence practitioners must have to perform specific roles and responsibilities. The EBK, coupled with role based training, will help develop a more highly skilled security workforce that is capable of responding to the dynamic and rapidly developing array of Cyber Threats / Attacks and Insider Threats.
- Conduct training requirements analysis, evaluation of training courses and review training course materials (Instructor / Student Guides, Course Activities, Handouts, Exercises, Exams) to ensure the content is complete, current, accurate and aligns with current NISPOM, CNSS and DoD requirements.
- Provide guidance and resources to DIB contractors on how to design, develop, implement, and maintain an Information Systems Security-Information Assurance Program.

Senior Information Assurance Manager-Engineer / Counterespionage Security Specialist

October 2009 To October 2011

DoD Insider Threat Counterintelligence Group (ITCIG)

Department Of Defense / Director Of National Intelligence (DNI) - Washington, DC, (Contractor: CACI)

- Assist the DoD ITCIG in establishing a comprehensive and structured DoD Enterprise Insider Threat Defense Program (ITDP) Risk Management Framework (RMF), that will integrate the security disciplines of Counterintelligence (CI), Security and Information Assurance (IA). The ITDP RMF will define the baseline activities to be conducted by DoD Combatant Commands, Services and Agencies to support their ITD Programs.
- Provide comprehensive risk mitigation strategies for the DoD Enterprise, in the areas of IA and Security (Management, Operational, Technical Controls), that will protect classified information, information systems and prevent espionage. Developed a DoD Insider Threat Defense Program Inspection Checklist covering CI, Security and IA. Conduct comprehensive audits of DoD organizations for compliance with various DoD directives, instructions, policies. Brief Senior DoD Leadership on Insider Threat risks, recent espionage cases, events and emerging trends.
- Research, evaluate and recommend various Computer Network Defense Tools and Data Loss Prevention Tools, to provide for the identification of malicious network activities or indicators of Insider Threats on DoD classified and unclassified networks.
- As a liaison to the DoD and IC community, work closely with the CNSS, DNI/ONCIX, FBI, CIA, NSA, DIA, DISA, DSS, DC3/DCFL, NRO, NGA, ARMY CI, AFOSI CI, NCIS CI on DoD and IC Insider Threat Defense Program development..

Designated Approving Authority Representative (DAA) / Certifier

March 2008 To October 2009

Department Of Energy, Office Of Intelligence/Counterintelligence - Washington, DC, (Contractor: Spectal)

- Reviewed Top Secret SCI Information Systems Security Programs, and JWICS Certification & Accreditation documentation for compliance with DCID 6/3, NIST, CNSS. Make Accreditation recommendations to the DAA.
- Performed vulnerability testing of operating systems and software applications using the following security tools; DISA Gold Disk, Nessus, Core Impact, Retina, Navy WASSP/SECSCN, Wireshark Network Traffic Packet Analysis etc.

Computer Forensics Investigator/Analyst

September 2007 To March 2008 (Short-Term Contract)

Central Intelligence Agency - Washington, DC, (Contractor: Brickner, Kelly & Associates)

- Performed Computer Forensics Investigations on Computers, Computer Media and Electronic Handheld Devices. Used a variety of tools to include; EnCase Forensics, FTK Forensics, Helix Forensics CD, Paraben's Device Seizure, Access Data Password Recovery Toolkit, Imaging Software and a variety of other Computer Forensics Software Utilities.
-

Director Information Systems Security / Designated Approving Authority Representative (DAA) / Certifier

April 2004 To September 2007

Defense Intelligence Agency (DIA) / National Media Exploitation Center (NMEC) - Washington, DC, (Contractor: Mantech)

- From the ground up, I developed, implemented and managed an Enterprise-Wide Top Secret SCI Information Systems Security Program for the NMEC, in accordance with various Federal Government, DoD and Intelligence Community regulations; OMB Memos, FISMA, Privacy Act, CNSS, DNI Special Publications, DCID 6/3, DCID 6/9, JAFAN 6/3, CJCSI 6510.01E, DoD 8500.2 IA, DoD 5105.21-M-1 SCI Admin Manual, NISPOM DoD 5220.22-M, DoD 5200.1-R Information Security Program, DoD 5240.06 Counterintelligence Awareness and Reporting, Joint DODIIS SCI Information Security Standards, DISA STIG's.
- **Other Major Responsibilities Included:** SSO/SCIF Accreditation and Management, Security Classification Guide and Security Policy Development, Conducted Enterprise Risk Assessments-Risk Mitigation, Managed the Certification/Accreditation of JWICS, SIPRNET, NIPRNET Networks, Configuration Control Board, Security, Education, Training and Awareness Program, COOP/Disaster Recovery Program and Computer Security Incident Response Team.
- **Promoted to DIA DAA Rep./Certifier.** Reviewed Top Secret SCI Information Systems Security Programs, Information Systems (JWICS) Certification & Accreditation documentation for compliance with DCID 6/3, JDCSISSS. Make Accreditation recommendations to the DAA. Use various software tools (DISA Gold Disk, Nessus, Retina, Navy WASSP/SECSCN, NetWitness Investigator Network Forensic Analysis Tool) to identify and test key security control points in the organization's network infrastructure and applications.

Information Systems Security Manager (ISSM)

October 2003 To April 2004 (Short-Term Contract)

Department Of Health And Human Services- Rockville, Maryland, (Contractor: ARTI)

- Developed, implemented and managed various Information Systems Security Program functions for the Department of Health and Human Services-Human Resources Services Division, servicing 65,000 HHS employee's nationwide.
- In accordance with the FIPS 199/200 and NIST SP 800-37, 800-53, 800-53A, performed Certification and Accreditation activities to include; Conducting Risk Assessments, Privacy Impact Assessments, developing System Security Plans, Contingency Plans. Performed Security Test and Evaluation. Managed POA&M Process.

Network Traffic Intrusion Analyst / Incident Response Manager

March 2003 To October 2003 (Short-Term Contract)

U.S. Special Operations Command- MacDill Air Force Base, Tampa, Florida, (Contractor: Dataline/EDS)

- Conducted detailed Network Traffic Monitoring/Analysis on USSOCOM Classified and Un-Classified Networks. (SIPRNET/NIPRNET). Performed the installation, configuration and administration of Securify SecurVantage Network Monitoring Appliances. Identified Suspicious And Malicious Activities, Worms, Viruses, Trojan Horses, Un-Authorized Connections Attempts Etc.). Reviewed Event Logs of various Network Monitoring Devices and Servers. Provided Incident Response Support (Impact, Damage Assessments, Recovery Actions / Procedures).

Director of Information Systems Security

March 1999 To March 2003

WSSC-State Government Public Water Utility- Laurel, Maryland

- Promoted from Network Engineer. Developed, implemented and managed an Enterprise Information Systems Security Program. Developed Policies, and Procedures, compliant with State/Federal Mandates and NIST/FIPS Special Publications.
- Per Presidential Decision Directive 63, and in conjunction with NSA, use NSA InfoSec Assessment Methodology to perform an Information Security Assessment of WSSC's Network Infrastructure. Reviewed information systems security postures to identify potential vulnerabilities and recommend steps for eliminating or mitigating those vulnerabilities.

Network Administrator

April 1998 To February 1999

Department of Justice ADCM Project- Silver Spring, Maryland, (Contractor: CACI)

- Responsible for the design, procurement, installation, administration, troubleshooting and repair of the ADCM Network. This TCP/IP Network was comprised of NT4 Servers, Exchange 5.5 Server and Windows 98/NT 4 Workstations.
- Developed, implemented and managed the Information System Security Program. Developed Security Policies, Procedures and Guidelines, and managed the Security, Education, Training and Awareness Program.

Network Administrator / PC Support Specialist

April 1990 To March 1998

Social & Scientific Systems- Bethesda, Maryland

- Responsible for the design, procurement, installation, administration, troubleshooting and repair of the Novell 3.12/4.11 and Windows NT 4 Server Network, supporting over 100 user workstations.
 - Installed hardware and software. Provided training and support for Windows 98 and Microsoft applications.
-

EDUCATION

- **High School Graduate**- Springbrook High School, Silver Spring, Maryland
- **Montgomery College**- Silver Spring, Maryland
Attended And Successfully Completed
 - Courses in Business Administration, Information Systems, Computer Science and Technologies Curriculums.

SPECIALIZED TRAINING (Continued)

- **Additional Training Courses**; SSO / SCI Security Officials Course, SCIF Inspector Training Course, Cross Domain Transfers-Hidden Data Course, Retina Vulnerability Scanner, FEMA Continuity of Operations Program Manager.
Courses Taught By; DIA, Navy, ManTech, DISA..

SPECIALIZED SKILLS

- Demonstrated ability to develop, implement and manage Federal Government / DoD Information Systems Security Programs.
- Demonstrated leadership skills, with the ability to successfully initiate, lead and manage individuals and multiple projects, from inception to completion.
- Demonstrated ability to communicate effectively (verbally and written) when briefing senior government directors and management, and when teaching Information Systems Security-Information Assurance Program Training Courses.

OUTSTANDING SERVICE AWARDS

- **Department Of Energy, Office Of Intelligence / Counterintelligence**: Certificate Of Appreciation / Cross Cutting Team Award - Outstanding DAA Service On Cyber Security Team / April 2008 and December 2008
- **ManTech Information Systems And Technology**: Meritorious Service Award / April 2007
- **DIA National Media Exploitation Center**: Recognition For Outstanding Service - SCIF Accreditation Project / April 2007
- **Director Of National Intelligence / DNI**: Recognition For Discovery & Cleanup Of Privacy Breach / May 2006
- **DIA National Media Exploitation Center**: Meritorious Service Award / May 2006