

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/ WITH FULL SCOPE POLYGRAPH

SUMMARY OF EXPERIENCE / RESPONSIBILITIES

- **15 Years of Hands-On Experience:** In the development, implementation and management of Enterprise Information Systems Security Programs/Information Assurance Departments, Insider Threat Risk Management Programs for the Department of Defense (DoD), National Level Intelligence Centers, Federal Agencies and State Governments.
- **Held Senior Level Leadership Positions As:** DoD Counterintelligence/Counterespionage Security Specialist, Information Assurance (IA) Subject Matter Expert, Designated Approving Authority Representative / Certifier Of Information Systems, Computer Forensics Examiner/Analyst, Senior Agency Information Security Officer (SAISO), Information Systems Security Manager/Officer (ISSM/ISSO), Director of Information Security, and SCIF Manager/SSO reporting directly to Senior Level Management and Directors.
- **DoD Counterintelligence / Counterespionage Security Specialist:** Provide Subject Matter Expert guidance and assist DoD Combatant Commands, Services and Agencies in developing, implementing and managing their Insider Threat Defense Programs (ITDP). Conduct audits of DoD ITDP's identifying weaknesses in Counterintelligence, Security, Information Assurance and recommending mitigation strategies. Define requirements, evaluate and recommend various IA Auditing, Monitoring, Investigation and Analysis Tools to detect suspicious or malicious behavior on DoD Networks. Provide Counterintelligence / Counterespionage and Insider Threat Defense Security Education Training and Awareness to DoD organizations.
- **Designated Approving Authority Representative/Certifier:** I performed Information Systems Security Program Reviews and Security Testing and Evaluation of Enterprise Top Secret SCI Information Systems/Networks and Software Applications. Ensure compliance with DCID 6/3, NIST 800-53 and CNSS Standards, Policies and Guidelines. Make recommendations for Accreditation.
- **SAISO And ISSM:** Implemented and Managed a Top Secret/SCI Information Systems Security Program for the DoD/Defense Intelligence Agency (DIA) National Media Exploitation Center. Responsibilities Included: Implementation of Management, Operational and Technical Security Controls per DCID 6/3, Oversee Certification/Accreditation of Information Systems, Manage Plan Of Action and Milestones (POA&MS) Process, Manage Configuration Control Board, Develop Policies and Procedures, Performed Risk Management and Insider Threat Risk Assessments, Manage the Security, Education, Training and Awareness Program and manage the Computer Security Incident Response Team.
- **Counterespionage / Information Systems Security Program Management Training Instructor:** I develop and currently teach a comprehensive Counterespionage Training Course to Security Professionals and an Information Systems Security Program Management Training Course / DNI ICD 503 to ISSM's/ISSO's for the Federal Government and DOD/IC Agencies.
- **Proficient With The Following:** DCID 6/3, DCID 6/9, DOD 8500.2, DOD 5105.21-M-1, NISPOM DOD 5220.22-M, DOD 5200.1-R, DOD 5240.06, Joint DODIIS/Cryptologic SCI Information Security Standards, JFAN 6/3, OMB A-130 Appendix III, FISMA, Privacy Act, NIST/FIPS Special Publications, NSA/DISA Security Technical Implementation Guides.

CERTIFICATIONS:

- **Certified:** CISSP/Certified Information Systems Security Professional
- **Certified:** Computer Forensics Investigator By NTI
- **Certified:** Securify Systems Engineer/ Network 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:** DOD Information Assurance Technology Analysis Center Subject Matter Expert (SME)

SPECIALIZED TRAINING

- **Raytheon InnerView / Insider Threat Focus Observation Tool (InTFOT) Investigator Training – Taught By Raytheon**
Topics Covered: InnerView allows observation of computer users who exhibit suspicious behavior, for analysis and identification of potential adverse insider threat activity. Covered Agent Creation, Policy Development, Investigations and Reporting.
- **Modeling Human Behavior In Cyberspace - Taught By DIA Behavioral Science Research**
Topics Covered: This training focused on the identification of Technical and Behavioral Counterintelligence and Security Risk Indicators. Discussed documented Insider Threat cases in government and industry. Provided knowledge to improve DOD Insider Threat Risk Detection and Mitigation capabilities from a Management, Operational and Technical controls perspective.
- **EnCase Computer Forensics Investigator Training Course - Taught By DIA National Media Exploitation Center**
Topics Covered: Acquisition, Examination, Analysis and Reporting of Digital Computer Media using EnCase Forensics Software.
- **InfoSec Assessment Methodology / Information Security Audits And Assessments-Taught By National Security Agency/NSA**
Topics Covered: How to conduct Information Security Audits and Risk Assessments of Information Systems.

I would appreciate having the opportunity to discuss with you in person my skills and abilities. I look forward to hearing from you. Please call 561-809-6800. References and Letters of Recommendation furnished upon your request.

Sincerely, James L. Henderson

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

PROFESSIONAL EXPERIENCE

DoD Counterespionage Security Specialist / Information Assurance SME

October 2009 To Present

DoD Insider Threat Counterintelligence Group (ITCIG)

Department Of Defense / DIA DCHC- Washington, DC

- The DoD ITCIG mission is to establish a comprehensive and structured DoD Enterprise Insider Threat Defense (ITD) Program Risk Management Model that will integrate the disciplines of Counterintelligence (CI), Security and Information Assurance (IA), and define the baseline activities to be conducted by DoD components for their ITD Programs.
- Provide Subject Matter Expert guidance and assist Combatant Commands, Services and Agencies in developing, implementing and managing their Insider Threat Defense Programs. Conduct audits of DoD organizations ITD Programs for compliance with DoD Insider Threat Policy and "Best Practices". Provide expert leadership and knowledge in the areas of Counterintelligence, Security and Information Assurance, with proven experience thwarting insider threat activities that could cause harm to the national security of the United States/DoD, through espionage, foreign terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities. Provide Counterintelligence/Counterespionage, Insider Threat Defense, Information Systems Security Education, Training and Awareness to DoD organizations.
- Representing the DoD ITCIG, serve as the IA Subject Matter Expert (SME) Liaison across the DoD and IC community. Work closely with the FBI, DNI/ONCIX, CIA, NSA, DIA, DISA, DSS, DC3/DCFL, NRO, NGA, ARMY CI, AFOSI, NCIS and other government organizations on Insider Threat issues. Evaluate and recommend various IA Auditing, Monitoring, Investigation and Analysis Tools to Detect, Deter and Mitigate Insider Threats to DoD Networks.
- Represent the DoD ITCIG at various Insider Threat Forums, Conferences, Working Groups and Meetings, across the DoD and IC community. Brief Senior DoD Leadership as necessary on significant Insider Threat problems, events and emerging trends, and provide structured and comprehensive risk mitigation strategies for improving national security and counterintelligence policies.

Designated Approving Authority Representative / Certifier

March 2008 To October 2009

Department Of Energy, Office Of Intelligence/Counterintelligence- Washington, DC

- Reviewed Top Secret/SCI Information Systems Security Programs and Certification and Accreditation documentation for compliance with DCID 6/3, NIST, CNSS Standards, Policies and Guidelines. Perform Security Test And Evaluation. Manage POA&M Process. Make Accreditation recommendations to DAA. Perform SCIF Inspections for compliance.
- Served as the Certification and Accreditation (C&A) Transformation Manager for the new DNI ICD 503 C&A Process. Provide Guidance and Training to DOE ISSM's and ISSO's on how to perform an orderly and smooth transition from DCID 6/3 to the new NIST and CNSS Standards, Policies and Guidelines.

Computer Forensics Investigator/Analyst

September 2007 To March 2008

U.S. Federal Government- Washington, DC

(Short-Term Contract)

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

Designated Approving Authority Representative / Certifier

April 2004 To September 2007

Senior Agency Information Security Officer / SAISO

Defense Intelligence Agency / National Media Exploitation Center- Washington, DC

- **DIA DAA Representative / Certifier:** Due to excellent job performance, promoted by DIA from an SAISO to a DIA Designated Approving Authority Representative/Certifier. Participated in Design Reviews, Technical Meetings and Security Testing/Evaluations to ensure/certify that the proper DCID 6/3 Security Controls were implemented in DODIIS Enterprise Top Secret/SCI Information Systems/Networks and Software Applications. Reviewed supporting documentation. Prepared Certification Test Reports, detailing Findings and Vulnerabilities. Made recommendations for Accreditation to Senior DIA DAA Officials.
- **NMEC SAISO Responsibilities:** From the ground up, I single handily designed, developed, implemented and managed an Enterprise Top Secret SCI Information Systems Security Program/Department, ensuring compliance with FISMA and various DNI/DIA/DOD/DCID regulations. Responsibilities Included: Policy Development/Implementation, Certification/Accreditation and Security Test/Evaluation of Information Systems/Applications, Managed Configuration Control Board, Performed Risk Assessments/Insider Threat, Managed Computer Security Incident Response Team, Performed SCIF Accreditation/Management, Performed Security Training/Briefings and assisted with COOP Development and Management.

Information Systems Security Officer / ISSO

October 2003 To April 2004

Department Of Health And Human Services / Rockville, Maryland

(Short-Term Contract)

- Was responsible for developing, implementing and managing the various Information Systems Security functions for the Department of Health and Human Services-Human Resources Services Division, servicing 65,000 HHS employee's nationwide.
- Performed Certification and Accreditation (C&A) activities to include conducting Risk Assessments, developing System Security Plans, and Contingency Plans. Performed Security Test and Evaluation and develop ST&E reports. Prepared C&A documentation for all Human Resources Services Information Systems in accordance with the NIST SP 800-37, 800-53, 800-53A, 800-60, 800-88.

Network Intrusion Analyst / Incident Response Support

March 2003 To October 2003

U.S. Special Operations Command / MacDill Air Force Base, Tampa, Florida

(Short-Term Contract)

- 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 Escalation/Support and Assess Probable Impact/Damages. Developed Course of Action and Recovery Procedures.

Director of Information Security

March 1999 To March 2003

WSSC-State Government Public Water Utility / Laurel, Maryland

- Developed, implemented and managed an Enterprise Information Systems Security Program. Developed Policies, and Procedures, compliant with State/ Federal Mandates.
- In conjunction with NSA, using NSA InfoSec Assessment Methodology, performed an Information Assurance Security Audit of WSSC's Network Infrastructure, reviewing Operational Systems/Technical/Physical/Administrative Controls.

Network Administrator

April 1998 To February 1999

CACI / Department of Justice ADCM Project / Silver Spring, Maryland

- 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 an Information Security Program. Developed Security Policies, Procedures and Guidelines.

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 NT 4 Client/Server Network, supporting over 100 Users running Windows 98 on the desktop computers.
- Installed Computers, Printers, Modems, Software. Provided Training/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, and Information Systems Curriculum
 - Courses In The Computer Science and Technologies Curriculum

SPECIALIZED TRAINING (Continued)

- Additional Training Courses; SSO / SCI Security Officials Course, SCIF Inspector Training Course, SCI ISSM / ISSO Training Courses, Information Assurance Security Officer Training Course, Cross Domain Transfers Course, Continuity of Operations Program Manager Training Course.
- Courses Taught By;** DIA, Air Force/Army/Navy and Federal Emergency Management Agency/FEMA.

OUTSTANDING SERVICE AWARDS AND SPECIAL ACCOMPLISHMENTS

- Federal Information Systems Security Educators' Association:** 2010 Security Training Course and Awareness Website Award
- Department Of Energy, Office Of Intelligence / Counterintelligence:** Certificate Of Appreciation / Cross Cutting Team Award For 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 For 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

SKILLS

- Demonstrated ability to Develop, Implement and Manage Federal Government Information Systems Security Programs/Departments, ensuring compliance with FISMA/DNI/DCID/NIST/CNSS/OMB regulations.
- Demonstrated ability to communicate effectively (verbally and written) in front of senior government directors and management.
- Demonstrated ability to initiate, lead and manage people and projects, from inception to completion.

PROFESSIONAL ORGANIZATIONS

- Member of The FBI Infragard Program-Maryland Chapter (Past Vice President)
- Member of the Federal Information Systems Security Educators' Association

NOTE: Certification / Training Certificates and Service Awards are available for review by request.