James L. Henderson / CISSP / CCISO

12119 Willow Wood Drive, Silver Spring, Maryland, 20904 • cybercops911@comcast.net • 561-809-6800

Current Security Clearance Level: Provided For Official Purposes Only

SUMMARY OF EXPERIENCE / RESPONSIBILITIES

- **15 Years Of Hands-On Experience:** In the development, implementation and management of complex Enterprise Cyber Security-Information Systems Security Programs, Information Assurance Risk Management Programs and Insider Threat Programs for the; DoD, National Level Intelligence Centers, Defense Industrial Base Contractors, U.S Government Agencies, State Governments, large and small businesses.
- **Leadership Skills:** Recognized as a seasoned security professional, who provides a practical approach to the security of data, information systems and risk management that meets both the needs and constraints of the organization. I have a proven track record of achievement, regardless of the technical, non-technical, and political challenges within an organization. Demonstrated team player, with the ability to successfully initiate, lead and manage individuals and multiple projects, from inception to completion. Ensure various divisions, departments and stakeholders are connected and communicating (HR, Physical / Personnel Security Legal, Cyber Security-IA, Etc.). This will provide a holistic enterprise risk management approach, eliminating silos.
- **Held Senior Level Enterprise Security Program Management Positions As:** Cyber Security-Information Assurance Program Management Training Course Instructor, Insider Threat Program Training Course Instructor**,** Insider Threat Security Analyst / Information Assurance Manager-Engineer, Cyber Security-Information Systems Security Program Manager, Continuity Of Operations Program 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 Business Management.
- **Cyber Security-Information Systems Security Program Manager Responsibilities:**
  From the ground up, I developed, implemented and managed an Enterprise Top Secret SCI Cyber Security-Information Systems Security Program for the Defense Intelligence Agency-National Media Exploitation Center. Protected the confidentiality, integrity and availability of mission critical classified-unclassified information and information systems. Apply defense-in-depth strategies using multiple layers of security; Physical / Operational Security, Network Perimeter, Application Layer, Storage Layer, Data Layer, End Points. **Major Responsibilities Have Included:** Security Policy and Security Classification Guide Development, Data Privacy Protection / Personally Identifiable Information (PII), Conducting Risk Assessments / Mitigation Guidance, Performing Certification / Accreditation of Classified / Unclassified Information Systems.
  Provide Cyber Threat Analysis / Information Systems Security Engineering Guidance In The Areas Of; Emerging Cyber Attacks / Threats, Malware, 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.
- **Cyber Security - Insider Threat Program Training Course Instructor-Consultant:** Develop and currently teach comprehensive Cyber Security-Information Assurance and Insider Threat Program Training Courses to security professionals for the Federal Government, DoD/IC Agencies, Defense Industrial Base Contractors, businesses and organizations. Provide briefings to organizations on the various aspects of Cyber Threats / Attacks and Insider Threats.
- **Proficient With Security Governance From:** NIST / FIPS Special Publications, Office Of Management And Budget Security Memos, Federal Information Security Management Act (FISMA), Privacy Act, DoD-Intelligence Community-CNSS Security Instructions-Polices-Procedures, SANS Consensus Audit Guidelines, Health Insurance Portability & Accountability Act (HIPAA), PCI Data Security Standards, FEDRamp Cloud Security, ISO, SOX, GLB, CobiT, ITIL.

CERTIFICATIONS / PROFESSIONAL MEMBERSHIPS AND RECOGNITION

- **Certified:** CISSP / Certified Information Systems Security Professional By ISC2
- **Certified:** Chief Information Security Officer (CCISO) By EC Council
- **Certified:** Computer Forensics Investigator By NTI
- **Certified:** Securify 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
- **Chairman:** FBI InfraGard / Maryland Insider Threat Special Interest Group (2011-2014)
- **Chairman:** National Insider Threat Special Interest Group (2014-Present)
- **Member**: Federal Information Systems Security Educators' Assoc. -Recipient 2010 Security Awareness Website Award
- **Recognition:** Information Assurance Subject Matter Expert - DoD Cyber Security-Information Systems /Analysis Center
- **Recognition:** American Society For Industrial Security Exceptional Performance Award 2012, For Support To FBI InfraGard / Maryland Cyber Security-Insider Threat Special Interest Group

James L. Henderson / CISSP / CCISO

PROFESSIONAL EXPERIENCE

Cyber Security Program Management / Insider Threat Program Training Course Instructor

February 2013 To Present

Top Secret Protection / Insider Threat Defense, Inc. – Silver Spring, Maryland (Independent Contractor)

- Design and develop Cyber Security-Information Assurance and Insider Threat Program Training Courses using the ADDIE Instructional Design Model and NIST SP 800-50: Building an Information Technology Security Awareness and Training Program.
- As a Cyber Security-Information Assurance and Insider Threat Program Training Course Instructor, I provide training courses to security professionals for the Federal Government, DoD / IC Agencies, Defense Industrial Base Contractors, businesses and organizations.
- The training courses are designed around the following security governance regulations and guidance; NIST / FIPS Special Publications, Office Of Management And Budget Security Memos, Federal Information Security Management Act (FISMA), Privacy Act, DoD, Intelligence Community, CNSS Security Directives and Instructions, National Insider Threat Policy, Health Insurance Portability & Accountability Act (HIPAA), PCI Data Security Standards.
- Provide consulting guidance and resources to organization on how to design, develop, implement, and maintain an Enterprise Cyber Security-Information Assurance Program and Insider Threat Program that protects Data, Information Technology Systems and Networks.

Cyber Security-Information Assurance Program Management / Training Course Instructor

October 2011 To February 2013

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

- Assist in the design, development and instruction of DSS (NISPOM Chapter 8), Cyber Security-Information Assurance 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 a Cyber Security-Information Systems Security Program Management Essential Body of Knowledge (EBK) that provides for a baseline framework of essential knowledge and skills that IT, IA, Security and Counterintelligence (CI) 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.
- Perform analysis of Cyber Threats, Insider Threat Attacks and Intrusions, Advance Persistent Threats and Malware. Provide countermeasures and training to mitigate the activities of Cyber Criminals and Malicious Insiders.
- Provide guidance and resources to DIB contractors on how to design, develop, implement, and maintain an Enterprise Cyber Security Programs and Insider Threat Programs that protect Data, Information Technology Systems and Networks.

Insider Threat Security Analyst / Information Assurance Manager-Engineer

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.
- Work closely with Intelligence Community Agencies (ICA's), DoD Commands, Services and Agencies (CSA's). Provided guidance and training to ICA's andCSA's to assist them with the establishment of an Insider Threat Defense Program for their organization.
- Research, evaluate and recommend various Computer Network Defense Tools, Data Loss Prevention (DLP) Tools and Security Information Event Management (SIEM) Tools to provide for the identification of malicious network activities or indicators of Insider Threats on DoD classified and unclassified networks. (Verdasys Digital Guardian, Raytheon Sureview, QRadar, Arcsight, Etc.)

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 DOE HQ 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.
- Conducted risk assessments of DOE National Labs. Provided Risk Mitigation Strategies.

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.

Cyber Security-Information Systems Security Program Manager
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, 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 Management Responsibilities Included:** Data Loss Prevention 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 Management, Security, Education, Training and Awareness Program Management, COOP/Disaster Recovery Program and Computer Security Incident Response Team Management.
- **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 COURSES

- NSA InfoSec Assessment Methodology / Information Security Audits And Assessments -Taught By NSA
- SCI ISSM Training Courses (Navy / Air Force), Army IA Information Assurance Fundamentals Training Course
- Raytheon InnerView-Insider Threat Focused Observation Tool Investigator Training - Taught By Raytheon
- DIA SSO / SCI Security Officials Training Course, DIA SCIF Inspector Training Course,
- Navy Hidden Data Training Course
- DISA Information Assurance For DoD Auditors And Inspector Generals
- DSS CDSE Training Courses:
  NISPOM Certification And Accreditation, Integrating Counterintelligence Threat Awareness Into A Security Program, Developing A Security, Education Training And Awareness Program, Introduction To Information Security, Cyber Security Awareness
- DHS Cyber Security For Industrial Control Systems
- Continuity Of Operation Program Management Training Course - Taught By FEMA

SPECIALIZED SKILLS

- Demonstrated ability to develop, implement and manage Federal-State Government, DoD and Private Sector-Business Cyber Security-Information Systems Security Programs and Insider Threat 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 Cyber Security-Information Systems Security Program Management 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 / 4-2008 and 12-2008
- **ManTech Information Systems And Technology**: Meritorious Service Award / 4-2007
- **DIA National Media Exploitation Center**: Recognition For Outstanding Service - SCIF Accreditation Project / 4-2007
- **Director Of National Intelligence / DNI**: Recognition For Discovery & Cleanup Of Privacy Breach / 5-2006
- **DIA National Media Exploitation Center**: Meritorious Service Award / 5-2006

References, Training-Certification Documentation Furnished Upon Request