

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/Departments for; Department of Defense, National Level Intelligence Centers, Federal Agencies and State Governments.
- **Held Senior Level Leadership Positions As:** 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, COOP Program Manager, and SCIF Manager/SSO reporting directly to Senior Level Management and Directors.
- **As A Designated Approving Authority Representative/Certifier:** I perform 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.
- **As A SAISO And ISSM:** Implemented and Managed a Top Secret/SCI Information Systems Security Program/Department for the 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, Perform Risk Management/Risk Assessments, Manage Security Awareness Training and Education Program and Manage Computer Security Incident Response Team.
- **Computer Forensics Investigator:** Perform Computer Forensics Investigations/Analysis in support of Department of Defense and Intelligence Community Anti-Terrorism Programs/Missions. Use EnCase Computer Forensics Software and a variety of other Computer Forensics/Security Tools to perform the Collection/Acquisition, Examination, Analysis and Reporting of Computer Media/Electronic Devices (Hard Drives, Floppies, USB Thumb Drives, PDA/Personal Digital Assistances, Cell Phones).
- **As An Information Systems Security Program Management Training Instructor:** I Develop and Currently Teach Comprehensive Information Systems Security Program Management Training Courses 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, Joint DODIIS/Cryptologic SCI Information Security Standards, JFAN 6/3, OMB A-130 Appendix III, FISMA, Privacy Act, NIST/FIPS Special Publications, DISA Security Technical Implementation Guides and NSA Security Configuration 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

### **SPECIALIZED TRAINING**

- **Designated Approving Authority / DAA Training Course– Taught By Defense Information Systems Agency/DISA**  
**Topics Covered-** This course covers all aspects of being a DAA. A DAA grants formal accreditation/approval to operate a system or network processing intelligence information. The DAA has the authority to withdraw accreditation, suspend operations, grant interim approval to operate, or grant variances when circumstances warrant.
- **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.
- **SCIF Inspector Training Course - Taught By Defense Intelligence Agency/DIA**  
**Topics Covered** – Provides SCIF Inspectors with advance knowledge of SCI Security (DCID 6/9, DOD 5105.21-M-1), identifying the Construction Standards and the Administrative/Physical Security Requirements to grant a SCIF Accreditation.
- **Continuity of Operations Program Manager Training Course – Taught By Federal Emergency Management Agency/FEMA**  
**Topics Covered** – Developing, Implementing, Managing and Maintaining a COOP Program for Federal Government Agencies.
- **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.

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

### Designated Approving Authority Representative / Certifier

March 2008 To Present

Department Of Energy, Office Of Intelligence/Counter Intelligence / Washington, DC

- Perform SCIF Site Inspections at Dept. Of Energy/DOE Field Intelligence Elements/FIES. Ensure SCIF's are in compliance with Top Secret/SCI regulations and procedures. Document areas of non-compliance, making recommendations for compliance.
- **Review Top Secret/SCI Information Systems Security Programs and Certification and Accreditation documentation for compliance with DCID 6/3, NIST and CNSS Standards, Policies and Guidelines. Perform Security Test And Evaluation. Manage POA&M Process. Make Accreditation Recommendations to DAA.**
- Serve 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. Mandate the use of the WASSP Security Testing Tool (SSO Navy) throughout DOE Enterprise. This drastically increased compliance with DCID 6/3 and NIST Windows Security Baseline Requirements.

### Computer Forensics Investigator/Analyst

September 2007 To March 2008

US Federal Government / Washington, DC

(Short-Term Contract)

- Perform Computer Forensics Investigations on Suspect Post-Mortem Computers, Computer Media and Electronic Handheld Devices. Use a variety of Computer Forensics Techniques to include: File Signature Analysis, Meta Data Retrieval/Analysis, Internet History Retrieval/Analysis and Keyword Searching. Also conduct Live Investigations.
- Recover Data on Computer Media/Electronic Devices from Deleted, Un-Allocated, Slack Space and Memory Dumps. Write Reports detailing Evidence Discovery for support of Internal and External investigations.
- Use a variety of tools to include; EnCase Forensics, ProDiscover Forensics, Helix Forensics CD, Paraben's Device Seizure, Access Data Password Recovery Toolkit and Imaging Software, WinHex 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, Managed Computer Security Incident Response Team, Performed SCIF Accreditation/Management, Performed Security Training/Briefings and assisted with COOP Development and Management.
- **Inter Agency Liaison:** The NMEC worked with many DOD and IC Agencies. (Director of National Intelligence/DNI, Central Intelligence Agency/CIA, DIA, National Security Agency/NSA, Federal Bureau of Investigation/FBI, Department of Defense/DOD, Department of Homeland Security/DHS, Defense Computer Forensics Lab/DCFL and others) I acted as the NMEC Liaison to these external agencies regarding all Information Security / Information Systems Security matters.

### Information Systems Security Officer / ISSO

October 2003 To April 2004

Department Of Health And Human Services / Rockville, Maryland

(Short-Term Contract)

- **Responsible for Developing, Implementing and Managing the Information 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 NIST SP800-26 Risk Assessments, developing System Security Plans, and Contingency Plans. Perform System Test and Evaluation and develop ST&E reports. Prepared into final format the necessary documentation for the C&A of 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

US 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. Identifies 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, complaint 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, 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.
- Managed the Procurement, Installation and Configuration of New Servers, Desktop Computers and Related Hardware.
- Developed, Implemented and Managed an Information Security Program, Security Policies, Procedures and Guidelines.

---

## Director of Information Systems Security

August 1990 To April 1999

### Garland Laboratory / Silver Spring, Maryland

(Consulting Position)

- Responsible for the Management/Administration of Corporate Network Information Systems ( Novell 3.12 / NT 4.0 Client/Server Network ). Managed the Budgeting and Procurement of Network Servers/Printers, Workstations, and other related H/W and S/W.
- Developed and Implemented a Corporate IT Security Program, Policies, Procedures and Disaster Recovery Plan.
- Conducted detailed Security Audits/Vulnerability Testing of Information Technology Systems/Networks. Developed Security Vulnerability Resolution Matrixes and manage the implementation of changes to correct vulnerabilities and mitigate risks.

---

## 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.
- Installed Computers, Printers, Modems, Software and 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)

- |  |   |
|--|---|
| ▪ SSO / SCI Security Officials Course                    | Defense Intelligence Agency/DIA         |
| ▪ Retina Vulnerability Scanner/Enterprise Manager        | Defense Information Systems Agency/DISA |
| ▪ SCI ISSM / ISSO Training Course                        | AFSCO/Air Force                         |
| ▪ SCI ISSM Training Course                               | Navy                                    |
| ▪ ISSM / ISSO Training Course                            | ManTech, Inc.                           |
| ▪ Information Assurance Security Officer Training Course | Army                                    |
| ▪ Hi-Low Security Domain Transfers                       | Navy                                    |
| ▪ Personal Electronic Device Vulnerability Briefing      | National Security Agency/NSA            |

## OUTSTANDING SERVICE AWARDS AND SPECIAL ACCOMPLISHMENTS:

- **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/DCID 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/NIPC Infragard Program-Maryland Chapter (Past Vice President)
- Member of the Federal Information Systems Security Educators' Association