

Christopher Alan Fitzhugh, CISSP, GCFA
3932 Triad Court, Woodbridge, VA 22192
Day/Work 202-586-5088
Home 703-586-7306
christopher.fitzhugh@in.doe.gov
fitzhughca@gmail.com

OBJECTIVE

Senior Information Security Engineer/Analyst

SUMMARY OF QUALIFICATIONS

- TOP SECRET/SCI clearance with CI Polygraph/DOE "Q" cleared
- Masters Degree in Information Systems
- Certified Information Systems Security Professional (CISSP) certification (#37516)
- 15 years experience in IT Security, COMSEC, Secure Communication and IT Audit fields
- SANS GIAC Certified Forensic Analyst (GCFA)
- DCID 6/3, DODIIS, DITSCAP Certification and Accreditation (C&A) documentation expert
- Extensive experience in UNIX Security, SRR Scripts, STIGs, resolving technical POA&M items
- Extensive experience in C&A of Controlled-Interface/Cross-Domain solutions
- Extensive experience in vulnerability assessment (NESSUS)
- Extensive Experience in penetration testing (CORE IMPACT, METASPLOIT and command-line)
- Experienced in Windows security (DISA Gold, CIS Benchmark), and resolving POA&M findings
- Expert in designing DCID compliant INFOSEC programs on a national scale
- Former military officer with extensive background in the intelligence community

EDUCATION

Masters, Information Systems, Webster University, 2001
Bachelors, Telecommunications, Loyola University, 1992

CAREER OVERVIEW

EDGEWATER INFORMATION TECHNOLOGY SOLUTIONS 2007-Pres

INFOSEC Engineer, DAA Representative, Office of Intelligence, Department of Energy

BAE SYSTEMS, NATIONAL SECURITY SOLUTIONS 2005-2007

Lead Systems Security Engineer, National Geospatial Intelligence Libraries

LOCKHEED MARTIN TECHNICAL OPERATIONS 2003-2005

Chief, Information Security, Defense CEETA

BAE SYSTEMS, INFORMATION SYSTEMS SECTOR 2002-2003

Information Systems Security Manager, DoD Systems

Christopher Alan Fitzhugh, CISSP, GCFA
3932 Triad Court, Woodbridge, VA 22192
Day/Work 202-586-5088
Home 703-586-7306
christopher.fitzhugh@in.doe.gov
fitzhughca@gmail.com

UNITED STATES AIR FORCE

1989-2002

Commander, 509TH Bomb Wing Network Operations Command Control Division

Commander, Combat Operations Command Control Division (C4ISR), 363rd Air Expeditionary Wing, Prince Sultan A.B., Saudi Arabia

Y2K Program Manager, Minot Air Force Base

Combat Operations Communication Squadron Leader, 401st Expeditionary Air Group

COMSEC Custodian, Top Secret Control Officer

Enlisted Terminal Attack Controller/Tactical Air Control Party

DETAILED EXPERIENCE:

INFOSEC Engineer, DAA Representative, U.S. Department of Energy, Office of Intelligence

Responsible for the overall security posture of the Field Intelligence Elements at the National Labs. Representative to the DAA for final accreditation of 25 systems. Act as liaison to DAA offices of other government agencies for the approval of major WAN connections in use at National Labs.

- Created and implemented an enterprise-wide Headquarters DAA Staff Assistance Visit program to ensure passage of Inspector General Audits. Program was tested under fire at the second-largest National Lab with excellent results. Designed program to be compliant with both the current DCID 6/3 and initial impending ICD standards based on current NIST methods.
- Forged a security agreement between the DOE Office of Intelligence and the National Nuclear Security Administration to ensure that DCID 6/3 was the governing regulation throughout the entire DOE Intelligence Enterprise. Resolution averted unnecessary expenditure of several million unfunded dollars.
- DAA Staff in charge of Accrediting, Testing and Security Implementation of a Presidential-Mandated, multi-million dollar program for the gathering, sharing and dissemination of sensitive nuclear material information across the entire IC.
- Created and implemented a security awareness training program for the entire DOE Intelligence enterprise. Training program was promulgated to 13 Field intelligence elements nationwide, providing training to over 6800 personnel.

Christopher Alan Fitzhugh, CISSP, GCFA
3932 Triad Court, Woodbridge, VA 22192
Day/Work 202-586-5088
Home 703-586-7306
christopher.fitzhugh@in.doe.gov
fitzhughca@gmail.com

Senior Security Engineer, National Geospatial Intelligence Libraries, Newington, VA.

Responsible for enterprise information security engineering of 22 government facilities in the greater Washington D.C. Metropolitan Area. Oversee and perform all measures of designing, documenting, testing and evaluating (ST&E) the entire enterprise architecture for DCID 6/3 compliance. Responsible for all program decisions involving compliance with the Federal Information Security Management Act (FISMA).

- Revitalized an ailing security program, receiving Approval to Operate (ATO) for 12 major networks in only 7 months time. No systems were correctly documented when I took over security for the program; all were fully documented less than 1 year later. Raised FISMA compliance for entire architecture from less than 10% to 100% in less than 1 year.
- Performed extensive security vulnerability testing of multiple sites to comply with DODIIS and DCID 6/3 standards. Implemented use of multiple host and network based vulnerability scanners, network mapping tools and exploit generation tools (NESSUS, NMAP, METASPLOIT, BINDVIEW) to create an enterprise-wide snapshot of vulnerability exposure. Efforts exposed previously unknown vulnerabilities and reduced exposure across architecture by 35% in less than 1 year in addition to ensuring that all existing system vulnerabilities were both known and documented.
- Created and implemented unique penetration testing strategies for high protection PL4 and PL5 controlled interfaces to ensure overall network safety during all phases of testing.
- Created, documented and established IT Disaster Recovery Plans for one-of-a-kind intelligence community networks at multiple locations in the Washington D.C. area
- Documented and certified secure remote access capabilities to monitor network security posture across the enterprise.
- Integrated security milestones into the overall project schedule for software rollouts. Ensured that performance of security hardening measures and vulnerability testing immediately followed installation of new software builds, resulting in no lapses in security.

Chief, Information Security, Defense CEETA, Springfield, VA.

Enterprise information security manager of a world-class U.S. Government datacenter. Completely overhauled all aspects of the program; raising the overall enterprise security posture threefold in less than two years.

- Established an ISO 9001:2000 and ISO17799 compliant enterprise information security program. Created information security policies to ensure compliance with headquarters directives while ensuring Federal Information Security Management Act (FISMA), and OMB regulatory compliance.
- Reduced enterprise-wide information security incidents by 42% in 2 years.
- Created an integrated DCID 6/3 compliance process across three major national sites to address undocumented legacy systems.

Christopher Alan Fitzhugh, CISSP, GCFA
3932 Triad Court, Woodbridge, VA 22192
Day/Work 202-586-5088
Home 703-586-7306
christopher.fitzhugh@in.doe.gov
fitzhughca@gmail.com

- Oversaw creation of 172 Certification and Accreditation (C&A) documents for the facility. Created a dedicated technical writing and security oversight staff where none existed before. System security posture and documentation was considered very high quality by DAA Representatives, with several systems carrying no liens, having received ATO far earlier than expected.
- Reduced incidents related to classified data spills by 88% through targeted education programs and policy enforcement. Nearly eliminated a problem plaguing the facility for 5 years.
- Created a Systems Administration training program to provide baseline security training for 269 admins spanning 4 states. Training was adopted as a best practice and implemented nationally.
- Procured emergency funding for creation of a \$50,000 annual IT security training budget for staff. After 1 year, all eligible staff members were CISSP certified. Expanded training budget to \$70K in 2004, addressing staff need for continuing professional education while cutting cost-per-session by 22%. Reduced staff turnover rates from an average of 1 per quarter to 1 per year.
- Drafted external security policy for vendors/suppliers wishing to enter into business contracts with the facility. Aggressively negotiated with vendor representatives to ensure compliance with DCID 6/3 equipment sanitization directives.
- Created and implemented a full-scale computer forensic capability to address proper conclusion of incident response measures. Forensics capability was tested under fire within the first 2 months of standup and performed flawlessly.
- Raised overall customer service standards within the information security group to new heights. Overall customer approval rating improved significantly from less than 20% to over 85% in six months. Recognized with a customer service excellence award for efforts.

Information Security Manager, Information Systems Sector, BAE SYSTEMS

Responsible for security policy implementation for a sector spanning 17 states. Acted as sole liaison to bridge the gap between DODIIS systems security and corporate network security policy. Ensured corporate INFOSEC compliance with NISPOM and State Department International Traffic in Arms Regulations (ITAR).

- Implemented SSL VPN solutions allowing secure hosting of employee services and network separation to satisfy State Department ITAR requirements between U.S. and Non-U.S. defense programs.
- Slashed corporate-wide downtime during the “Blaster” and “Welchia” worm incident to 1/10th of the “Slammer” worm incident. Saved a \$750 million, 10 year sales contract in the process. Personally commended by IT Director for my actions.
- Incorporated security into enterprise computer imaging program. Integrated security updates and service packs into a quarterly rollup to ensure compliance with corporate network security policy.
- Implemented facility plan for secure storage and retrieval of backup media as part of an overall disaster recovery strategy

Christopher Alan Fitzhugh, CISSP, GCFA
3932 Triad Court, Woodbridge, VA 22192
Day/Work 202-586-5088
Home 703-586-7306
christopher.fitzhugh@in.doe.gov
fitzhughca@gmail.com

Consolidated Career Events and Awards as United States Air Force Officer/Enlisted

Various leadership positions culminating in the command of a 100-person network operations center serving an 8,000-person United States Air Force base.

- Created an IT best practice disaster recovery and business continuity plan used throughout an entire command of 250,000 personnel.
- Hand selected as program manager for Y2K testing of 150 nuclear missile sites. All stages of the 2 year, \$25 million project were completed under budget and assured 100% mission success. Unit received a Presidential citation for outstanding achievement for the effort. Personally awarded the Air Force Commendation Medal for efforts.
- Senior Inspector General (IG) assessor for classified systems penetration testing and vulnerability assessment “red-team” message intercept groups during worldwide nuclear command and control exercises.
- Created, designed and field-deployed forward combat operations C2, C3, C4I and C4ISR communication networks during combat tours in Afghanistan, Iraq and the Yugoslavian Theater of Operations.
- Received Air Force Commendation Medal for saving the lives of five Airmen when a tornado destroyed a missile facility under my command.
- Awarded 8th Air Force Instructor of the Year for creating computer based INFOSEC training modules.
- Extensive ground combat experience in providing Tactical Air Control (TAC) to Army Special Forces units in multiple locations in active Areas of Responsibility (AOR).