TOP SECRET / SCI

Andre Tarry

dretarry@gmail.com | 618-969-5711

**Certifications & Training:**

12 years multi perspectives within cyber security

CompTIA Security+ Certification

ICD-503 XACTA User Training Certification

NIST 800-53 standards

Top Secret Security Clearance (SCI/Poly)

Currently studying for the CASP

**Professional Summary:**

IT Security Analyst over 12 years combined experience providing internal and external customers with the technical infrastructure necessary to meet, configuration management and exceed complex operational needs. I have experience in information assurance performing analysis of compliance vulnerabilities, mitigation of vulnerabilities, and audit related activities in a classified environment. I have seven years of compliance experience with the Nationals Institute of Standards and Technology Special (NIST) Publications 800-53, ICD 503, and ISO and formal risk management processes. I work closely with cross functional teams, government team leads, and testers to gather and document requirements, facilitate team meetings, lead briefings, and stakeholder communications; create documentation of risk/vulnerability, policies, and resolution. I leverage excellent communication skills for effective teamwork and works well with all levels of an organization to build consensus; possesses the ability to work in a fast- paced environment with multiple priorities.

**Key Skills Summary:**

|  |  |  |
| --- | --- | --- |
| **Security Frameworks:**  | **Security Analysis:**  | **Business Analysis:**  |
| NIST 800-53 | Risk Assessments | Requirements Gathering |
| ICD – 503 | Vendor Evaluations | Communication |
| DCID 6/3 | Security Assessments | Process/ Policy and Procedures |
| ISO | Audits | Coordination |
| Risk Management Framework (RMF) | Best Practices | Project Documentation |

**Professional Experience:**

* Conducted Cyber IT Security Assessment of TVA’s compliance with NIST Special Publication 800-53 for Information Security at hydro-electric plants and supporting IT areas.
* Assisted with the assessment of 28 hydro power generation dams, 1 pumped storage power generation system and 2 control centers.
* Interviewed critical personnel at all of the sites as well as senior management, including the review of policies and procedures and artifacts of compliance.
* Assisted in the development of 9 reports including the data, findings and recommendations related to all assessments.
* Trained via Air Force on networking. Led projects, gave briefings to and made reports to leadership.

**RMF Security Control Assessor / Bylight Scott AFB March 2020 – Present**

* Responsible for assessing the management, operational, assurance and technical security controls implemented on eMass information systems via security testing and evaluation methods compliant to NIST and RMF.
* Interview program managers for control review and compliance
* Perform STIG checks and vulnerability scans for ATO package submitals

**RMF Security Control Assessor / Unit SOJTF-OIR Camp Arifjan Kuwait March 2019 – March 2020**

* Responsible for assessing the management, operational, assurance and technical security controls implemented on eMass information systems via security testing and evaluation methods compliant to NIST and RMF.
* Performed system development, operation and deficiency mitigation.
* Performed system registration within eMass

**RMF Security Engineer Paragon / Scott AFB, IL**

 **May 2018- Nov 2018**

* Advise customer on aspects of certification and accreditation tasks for various IT systems.
* Assist IT systems in the development of security documentation, security test plans, security testing, analysis of results, and adequacy of risk assessment reports documenting vulnerabilities, threats, impacts, and recommended mitigations.
* Review IT system documentation and assess applicability, accuracy, and completeness in satisfying security controls, and document results and recommendations.
* Work with a certification team including data owners and systems administrators to gain in-depth knowledge of complex networks to ensure system authorization documentation accurately depicts the environment.
* Review contractor-produced security deliverables including system documentation, security test plans and procedures, and other artifacts for accuracy to validate system compliance with Department of Defense and Federal security requirements.
* Participate in technical meetings covering a broad range of system analysis, design, and security topics.

**ISSO Link Simulation and Training / Altus AFB, OK 3/2018- May 2018**

* In support of Department of Defense and National programs. I am responsible to the ISSM for the program System Continuous Monitoring, Plan of Action and Milestones (POA&M), Vulnerability scans, and other general security related duties.
* Work with the program team and government customers to determine and develop an approach to information system security solutions to meet contractual security requirements.
* Held the role of the cybersecurity point of contact and coordinate security compliance for the site.
* Responsible for coordinating activity with the site team including, appropriate security measures, identifying potential security weaknesses, recommending improvements to address vulnerabilities, and monitoring system security.

**ISSO ALTA IT Services / FBI Detroit, MI**

**Oct/17- Jan/18**

* Establishes audit policy and reporting mechanisms for ensuring compliance with IA/IS standards by keeping current with IA/IS requirements and RMF
* Analyze identified security strategies by assessing them against the organization's needs and compliance guidelines and selects the best approach or practice for the enterprise.
* Lead the development of risk management by creating plans, procedures, protocols, and evaluation measures and ensuring there are desired levels of enterprise-wide IA/IS compliant to NIST standards.
* Oversees the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.

**DISA Operational Engineer, Scott AFB IL**

**Nov/2016 – March/2017**

* Use network monitoring tools to identify problems and help customers requiring assistance with network hardware, software, or inquiries.
* Configuration management; tracking and controlling changes in software used.
* Provide problem determination/resolution based upon personal experience, expert opinion and standard operating procedures, including immediate resolution where possible.
* Work with other network technologists that are involved in network monitoring and maintenance, configuration management, compliance with NIST documentation and customer support.
* Document and propose solutions for network problems and work with appropriate personnel to achieve resolution.
* Participate in resolution of service-related issues.
* Interface with users and support organizations to ensure smooth flow of communications in all directions.
* Extensive network integration for a variety of network protocol standards, analyzing VLAN, routing, IP Addressing and sub-netting. (Prior contracts with TACC)

**DTSI COMSEC Analyst, San Antonio Texas, Kelly Port San Antonio HNCDK**

**June/2015 – Aug/2015**

* Responsible for supporting government personnel in the execution of transitioning DoD COMSEC Accounts to Key Management Infrastructure (KMI) Operating Accounts.
* Coordinate with stakeholders to ensure network firewalls are operational to support the KMI Virtual Private Network (VPN) connections
* Configure High Assurance Internet Protocol Encryptor (HAIPE) to KMI specifications
* Assist in the ordering, receipt, and usage of COMSEC Keys required for account transitions
* Prepare DoD COMSEC account database for transition to the KMI Management Client (MGC)
* Assist in completion of account inventory actions and resolving technical issues
* Monitor, track, and support COMSEC account inventory activities IAW National Security Agency (NSA) and service level policy
* Provide KOAM technical assistance for the installation of the KMI MGC node HW/SW and the transition of the COMSEC account data to the KMI MGC
* Monitor and track account installation progress and collaborate with COMSEC account personnel to resolve any transition issues
* Hand off long-term support responsibility to the Technical Support Center (TSC) after transition and installation is complete and all outstanding issues are resolved

**National Geospatial-Intelligence Agency St. Louis MO, Lackland AFB TX, Joint Operation Warfare Center, Information Security Engineer CACI, Inc. June/2013 – May/2015**

* Lead organization with the transition from DCID 6/3 to become compliant with the ICD 503 system accreditation process and RMF.
* Reviews complex System Security Authorization Agreements/ System Security Plans and Plans of Actions and Milestones (POA&Ms) documentation for new system initiatives.
* Reviews network policy and security requirements to ensure compliance with guidelines established by National Geospatial-Intelligence Agency and associated agencies.
* Utilizes Certification and Accreditation (C&A) collaboration tools to obtain system Operational Approvals to Test (OATTs), Approvals to Operate (ATOs), Approvals to Connect (ATCs), and Approvals to Proceed (ATPs).
* Monitors Information Technology (IT) equipment implementation and configuration and timely Vulnerability Assessment Testing (VAT).
* Utilize Director of Central Intelligence Directive (DCID) 6/3 and Intelligence Community Directive (ICD) 503.
* Mirrored testers during vulnerability scans for all systems seeking certification and accreditation. Would also make decisions based on results of the tests or scans.
* Involved in building the ICD 503 process from the ground up
* Perform penetration testing to identify vulnerabilities in Web Applications, Operating Systems, Network Equipment, Wireless, Mobile, and Databases.
* Utilize knowledge of security and network infrastructures including switches, routers and firewalls; TCP/IP networking, Microsoft Exchange, and Active Directory.
* Performed tasks associated with safeguarding the organization’s information systems with a focus on risk analysis, and Federal and organizational policy compliance by conducting Information Assurance security assessments, performing NIST-based risk assessments with many security relevant controls, and providing authorization recommendations; performing risk management and risk assessment, with system monitoring tools like XACTA.
* Reviewed network policy and security requirements to ensure compliance with the NIST-based guidelines established by associated agencies.
* Created a checklist for security system control, helping to identify security relevant controls.
* Created an Authority to Operate letter
* Notable accomplishments include:
* NIST 800-53 Audit

**US Air Force - Lackland Air Force Base, TX Record COMSEC Manager Aug/2012 – June/2013**

* Provided timely, effective, and comprehensive ordering, accounting, receiving, and distributing Communication Security Keying Material.
* Utilized Information Assurance expertise for Keying Material. Responsible for receiving, processing, and recording orders from/to Central Office of Record. Ensured all accounting and tracking of information within Central Office of Record was contained within the COMSEC Accounting, Reporting, and Distribution System (CARDS).
* Documented and tracked KEYMAT inventories and deliveries.
* Provided status reports on a periodic basis.
* Investigated, tracked, and resolved KEYMAT distribution issues.
* Documented and tracked resolution of COMSEC account issues from creation through final disposition.
* Provided on-call support to enable priority emergency KEYMAT support to continue without interruption.
* Provided feedback on training and testing of future key distribution systems.

**Illinois National Guard- Scott Air Force Base, IL Cyber Security Manager Aug/2008 – Aug/2012**

* Operated, repaired, and deployed IT resources to monitor (Security Key Loader, 1553 & 283 communicative documentation)
* Evaluated and maintained systems, policy, and procedures to protect clients, networks, data/voice systems and databases from unauthorized activity
* Administered and managed the overall Information Assurance (IA) program to include COMSEC, Emissions Security (EMSEC) and Computer Security (COMPUSEC) programs
* Facilitated briefings and classes explaining the operations of equipment on the aircraft to high level executives
* Provided VOIP phone system support experience