# TRACEY B. MANUEL: PHD, CISO, CISSP, SPC (SAFE6)

Veteran IT professional with over 25 years of experience in design and verification of major architecture and data information management systems for IT Portfolio in a distributed development environment. Lead Agile teams in establishing design constraints, evolving identity and Access Management programs, and ensuring architecture conformed to established requirements through life cycle management processes. Significant experience in drafting data and information management products and service standards along with testing and evaluating (assessments) impacts of security decisions into the product and service lifecycles. Additionally, spent numerous years implementing and managing security standards and strategies for organizations. Served as lead security professional for many programs and projects, providing strategic vision and implementation. Excelled at providing analysis and evaluation as new technologies emerge, and training teams in agile work environments.

## EDUCATION

**SPC,** Certified SAFe® 6 Practice Consultant – 08/2023
**PhD,** Organizational Leadership and Development, University of Arizona Global Campus – 11/2021
**Master of Science**, Management Information Systems and Technology, Capella University - 2017
**Master of Science**, Management Information Technology, American InterContinental University - 2004
**Bachelor of Science**, Management Information Systems, Auburn University - 1998
**Military Leadership Training**, Captains Career Common Course, Command, and General Staff College
Trained as a Cisco Networking Academy Instructor 2003

## CERTIFICATIONS/CLEARANCES

**C|CISO** - Certified Chief Information Security Officer; **CISSP** - Certified Information Systems Security Professional **Security+** - CompTIA; **Network+** - CompTIA; CEH –Certified Ethical Hacker; **A+** - CompTIA; SAFe certified; **TS Clearance**

## AREAS OF EXPERTISE

- Cyber Threat Analysis/Modeling
- iCloud
- Network Administration
- Agile Management
- DIACAP/COBIT/SOX/NIST/PCI
- IT Governance
- Emergency Response
- IBM DOORS
- Code Analysis
- Project Management
- Disaster Recovery Planning/Testing
- Risk/Privacy Assessments
- Certification/Accreditation
- Strategic Planning
- Application Security/Assessments
- BORIS
- Software Development Life Cycle
- Relationship Building
- Static/Dynamic application security testing
- Leadership
- Technical Training
- Data Privacy/Protection
- SIEM Tools

## KEY SKILLS ASSESSMENT

**STRATEGIC PLANNING AND POSITIONING** – Collaborate with cross-functional teams for strategy planning activities, focusing on short and long term IA solutions with an emphasis on efficiency, budget, flexibility, and stability.

**INFORMATION ASSURANCE/SECURITY SUBJECT MATTER EXPERT** – Evaluate, analyze, and implement security solutions and emerging security technologies, aligning with future vision of organization infrastructure and IT best practices. Experience with Java, C++, FORTRAN, Visual Basic, and SQL.

## PROFESSIONAL EXPERIENCE

**SECURITY 1ST CONSULTING,** MONCKS CORNER, SC MAY 2016- PRESENT
**PRESIDENT & CEO**

- Guides company practices and procedures
- Oversees company operations, communications, and makes important decisions that impact the company's brand identity and financial health

- Acts as spokesperson for the company
- Writes proposals
- Develops strategic policies
- Assists in recruiting, onboarding, and training key personnel
- Manages the organization's budget
- Identifies new business opportunities

**FAVOR TECHCONSULTING,** VIENNA, VA NOVEMBER 2021- PRESENT
**CYBER INFORMATION SECURITY LEAD**

- Provides overall Cyber Security for FEMA RTPD systems
- Supports the protection of the systems and data within the program and helps maintain the system ATO
- Provides oversight to the software development teams in terms of cyber security
- Works closely with the Government staff on the cyber security design and maintenance
- Safeguards information system assets by identifying and solving potential and actual security problems
- Evaluated/ configured IP LAN and/or 802.11 Wireless LAN Systems on Cisco, Juniper, and Brocade hw
- Protects system by defining access privileges, control structures, and resources
- Recognizes problems by identifying abnormalities, reporting violations
- Implements security improvements by assessing current situation; evaluating trends; anticipating requirements
- Determines security violations and inefficiencies by conducting periodic audits
- Upgrades system by implementing and maintaining security controls
- Keeps users informed by preparing performance reports; communicating system status
- Maintains quality service by following organization standards
- Maintains technical knowledge by attending educational workshops; reviewing publications
- Contributes to team effort by accomplishing related results as needed
- Creates/updates POA&Ms and ISA documents as needed

**GEORGE CONSULTING, LTD,** CHARLESTON, SC OCTOBER 2018- NOVEMBER 2021
**SENIOR CONSULTANT**

- Supported Department of Education (DOE) by assisting in the development of strategic plans and supporting Risk Management and ATO development for applications, electronic systems, and other computing devices
- Supports USMC MSO by providing thought leadership for cloud brokerage and migration services
- Responsibilities include evaluating current USMC cloud migration processes and identifying instances where those processes can be improved upon
- Works on Authority to Operate and Authority to Connect packages for MSO applications, to include developing system documentation, architectural diagrams, system security plans, continuity of operations plans, system recovery, vulnerability and security control assessments, and disaster planning
- Works on RMF packages for Marine Corps, utilizing DISA STIGS / SRG checklists in a GovCloud environment
- Provides analysis of alternatives for potential cloud hosting providers
- Responsible for providing cost guidelines to assist customers in determining their potential rent cost for migrating their apps into various cloud environments
- Responsible for creating processes and procedures to increase efficiencies around cloud migration determinations
- Setup wireless network and upgraded Lan using Cisco equipment.
- Evaluated IP configurations on Aruba and Brocade equipment
- Responsible for identifying automation to replace manual processes used in cloud migrations
- Serves as Scrum Master for team

**TECHSOFT,** CHARLESTON, SC AUGUST 2016- SEPTEMBER 2018
**SENIOR CYBERSECURITY MANAGER**

- Supported the National Science Foundation (NSF) and SPAWAR Office of Polar Programs (SOPP) by providing thought leadership in many areas to ensure the security of systems all over the world

- Responsibilities included evaluating and identifying effective risk management (RMF) procedures using NIST/RMF guidelines, STIG,s/SRG checklists, Navy guidelines, and other industry best practices
- Provided cybersecurity controls management using governance documents and identifying training requirements
- Responsible for security validation through physical scans, interviews, and document reviews of all SOPP systems; which includes locations in North Charleston SC and Antarctica
- Worked with other leaders throughout SPAWAR and NSF to develop better risk metrics and risk reporting capabilities
- Evaluated IP configurations on Cisco and Aruba equipment
- Provided support by reviewing systems engineering designs, systems analysis and hardening, vulnerability testing, security test and evaluation, and policy analysis/updates for systems, computers, and network devices
- Applied knowledge of technology, analyzes security posture and its subsequent implications and provides recommendations in formal reports after annotating results and acquiring evidence to support findings
- Identified mitigations and recommendations to protect systems while also ensuring their confidentiality, integrity, availability, authentication, and authorization.
- Applied knowledge of NIST validations to assist technical projects in attaining an acceptable security posture
- Worked with third party providers to increase identity and access management, especially with the increased use of mobile devices (BYOD) as communication systems
- Assisted with the IA component of strategic planning and documenting IA strategies for future system implementations, including developing architectural diagrams, continuity of operations plans, system recovery, system security plans, vulnerability and security control assessments, system documentation, and disaster planning

**BOEING,** OKLAHOMA CITY, OK DECEMBER 2015-AUGUST 2016

**SYSTEM SECURITY ENGINEER LEVEL 5**

- Applied advanced job principles, theories, and concepts to provide solutions and recommendations to risk management issues using NIST guidelines and DISA STIG's to assess and evaluate computer systems, communication systems, and other electronic communications devices aboard aircraft
- Identified system set requirements and provides strategic designs of enterprise architectures for the Air Force
- Interjected application security into business requirements without adversely affecting desired functionality
- Ensured system and architectural designs conform to operational and system requirements
- Developed documentation, including security control assessments, security assessment reports, vulnerability assessments and plans, disaster recovery plans, and continuity plans to support ATO/ATC for applications on Air Force networks, to include computer, electronic, and communication systems
- Contributed to the development of new principles and concepts as well as advanced job practices, techniques, and standards
- Worked on unusually complex technical problems and provides solutions which are highly innovative and ingenious
- Initiated assignments and determines and pursues courses of action necessary to obtain desired results
- Collaborated with developers to perform static/dynamic code analysis tools such as Klocwork and Parasoft to analyze and mitigate software vulnerabilities
- Developed advanced technical ideas and guides their development throughout the software development cycle into final product
- Designed and working with enterprise architecture designs to include NAS/SAN storage for aircraft, Fibre Channel switches, and HBSS
- Served as organization spokesperson on advanced projects and programs by providing strategic vision and direction to ensure that system designs are in compliance with business and technical needs
- Acted as advisor to management and customers on advanced technical research studies and as a mentor/trainer to peers and subordinates
- Evaluated and test security, data protection, and performance planning standards against new technologies and concepts to identify solutions to design and produce solutions to high level complex problems
- Evaluated Ip configurations for wired and wireless systems utilizing Cisco and Juniper equipment
- Worked with third party vendors, contractors, and government employees to ensure that identity and access management are implemented in new system designs being incorporated into military aircraft

**AGILEX/ACCENTURE FEDERAL SERVICES,** CHARLESTON, SC July 2014–DECEMBER 2015

**TECHNICAL DIRECTOR/DIRECTOR OF OFFICE ADMINISTRATION**

- Oversees the development of mission-critical applications and technology to support long-term goals
- Worked as an IT Technical Director to expand design specifications into workable solutions and guide project teams

- Responsible for identifying, testing, and evaluating emerging information technologies to be assimilated and integrated within the VA organization for network and communication devices
- Responsible for identifying operational and system requirements needed to successfully execute Enterprise Information Systems program, estimate activity duration, and develop schedules/staffing plan
- Helps guide senior management and project teams during the technology decision-making process
- Effectively explains technical capabilities and features in business terms and generates management support required to deliver an organization's technology strategy
- Drives the development of best practices throughout the organization, while governing control and ensuring objectives are achieved
- Experience with server hardening, configuration compliance, static and dynamic code analysis and vulnerability management using various tools, such as (USGCB/FCC, DISA STIG, GPO, etc.) of computers and electronic systems
- Recommended solutions to Enterprise problems associated with VA systems in a cloud environment
- Provided leadership in the development of documentation to support system ATO/ATC, including architectural diagrams, continuity plans, configuration management plans, system security plans, security assessment plans, and disaster recovery plans.
- Thrives in Agile environments and able to manage multiple tasks/projects
- Worked in a Distributed Development Environment producing advanced technical designs and ensuring software security on computers, routers, switches, and other electronic communication devices
- Planned, developed, implemented, and evaluated information systems/applications and validated security of those applications using NIST guidelines and RMF guidance.
- Evaluated and configured IP configurations for IP networks using Cisco and Aruba equipment
- Experience leading information systems projects in healthcare environment
- Managed the overall daily operations of Charleston branch of Agilex
- Worked to improve processes and policies, managed administrative staff, and helped define long-term organizational planning
- Primary liaison to building landlord, overseas network administration, manages phone system, and works with HR on staffing efforts for several IT portfolios in the Charleston area

**L3/ENGILITY,** CHARLESTON, SC May 2012–July 2014

**INFORMATION ASSURANCE/INFORMATION SECURITY MANAGER**

- Accomplished at performing full DIACAP/NIST/RMF based Certification and Accreditation (C&A) efforts to include ATO's/ATC's of routers, switches, servers, OS's, and various other electronic communication systems
- Responsible for identifying system and operational requirements needed to successfully execute the information systems program, estimate activity duration, and develop schedules and staffing plans
- Experience performing Privacy Impact Assessments (PIA) and knowledge of best practices protecting Personally Identifiable Information (PII) and Protected Health Information (PHI)
- Experience directing, evaluating, and testing remediation efforts, building Residual Risk Reports, creating security impact assessments (SIA's), and creating/managing POA&Ms
- Practical experience using Nessus, Retina, Splunk, Symantec, Tripwire, Fortify, Rapid7, Gold Disk, SRR scripts, Wireshark, STIGs, Nmap, and AppScan to asses security vulnerabilities on various electronic systems
- Established metrics, key performance indicators, and service level agreements to drive system performance and trends
- Collaborated with customers to identify, develop, and implement strategic plans and system/operational requirements that provided added protected threats
- Evaluated applications against OWASP findings and performed automated analysis and mitigations using fortify and klocwork
- Responsible for ensuring that IP configurations were correct on Cisco and Juniper equipment
- Developed supporting documentation for system accreditation packages to include, system security plans, security control assessments, disaster recovery plans, continuity plans, and configuration management plans.
- Implementing Agile (Scrum) methodologies into IA daily activities
- Examined audit trails to ensure systems logs were created and reviewed according to audit plans and regulatory guidance
- Familiar with IA Best Practices relating to the following technologies; cloud, Windows Operating Systems, Oracle/WebLogic Databases, Web Technologies, Network Infrastructure, Hardware Virtualization, Unix Operating Systems, and storage (NAS/SAN)
- Recruited, trained, and mentored IA staff as well as conducted and oversaw internal system audits

**SCL SERVICES,** MT. PLEASANT, SC October 2009-May 2012

**SENIOR INFORMATION ASSURANCE ENGINEER**

- Served as Project Manager/team lead, responsible for planning, directing, and implementing information technology policies and ensuring configuration management of systems
- Interpreted DoD IA policies and provide IA support for U.S. Navy, Marines, and Army systems
- Evaluated and implemented application/software security best practices, performed code review, and mitigated findings using tools such as retina, Gold disk, STIGs, and OWASP for computer and electronic systems
- Administered, troubleshot, and assessed networking devices in a cloud environments, including NAS, SAN, and KVMs
- Prepared RFPs, analyzed proposals, recommended purchases, selected services, and managed new approaches in development processes
- Worked with military entities to create and refine operational and system requirements and implement them into their existing governance
- Performed Independent Verification and Validation (IV&V) testing of systems to ensure adherence to FISMA and other regulatory guidelines
- Evaluated IP configurations on wired and wireless networks using Juniper and Cisco equipment
- Created, updated, and maintained C&A artifacts to include; System Security Plans, Incident Response Plans, Security Test & Evaluation Plans, Contingency Plans, Risk Management Plans and Vulnerability Management Plans using RMF/NIST/DIACAP/PCI/SOX as guidelines
- Created and managed the remediation/mitigation of system vulnerabilities and conducted non-invasive pen tests of systems
- Developed IA staff capabilities through training and restructuring according to knowledge, skills, and abilities of team members
- Exposed to European data protection laws while working with personable identifiable information in systems in Germany
- Experience working with networking concepts and troubleshooting devices (routing/switching/IDS/IPS, firewalls)

**EAGAN, MCALLISTER & ASSOCIATES/SAIC,** CHARLESTON, SC October 2003-October 2009

**SYSTEMS INFORMATION ANALYST II** (2008-2009)

- Shift lead responsible for improving situational awareness of Navy Medicine networks and providing technical and subject matter expertise (SME) to assist with administration of network security devices, including cisco routers and switches
- Responsibilities included identifying and analyzing operational and system requirements for networks
- Provided innovative information systems services to projects through effective and efficient program management, ensuring the privacy of customers and compliance to state and federal regulations
- Managed perimeter security for 26 global sites, which included 26 Cisco 7200/3800 perimeter routers, Cisco 6509 FWSM, Cisco PIX/ASA firewalls, McAfee sensors, IDS monitors, and Fibre Channel switches
- Daily duties included log analysis, STIG reviews, testing, evaluating, and maintaining router configurations, and updating documentation of computer and communication systems
- Developed working relationships with customers and employees, facilitating the resolution of problems
- Provided strategic IT direction, management of project phases, and training to customers and end users
- Mitigated issues, potential risks, and deficient audit results through on going system analysis and security reviews

**INFORMATION SECURITY ANALYST IV** OCTOBER 2003- OCTOBER 2008

- Served as team lead of 3-4 personnel, deployed internationally to facilitate healthcare systems upgrades
- Worked with customer to identify operational and technical systems requirements
- Tested/evaluated the functionality of the IT infrastructure, architectural designs, and identified issues, potential risks, and audit results
- Provided installation, support, and training for Composite Health Care Systems (AHLTA) worldwide
- Configured and installed Windows 2000 servers, workstations, Internet Information Servers, and Tardis.
- Monitored network traffic, reviewed configurations, and conducted research on network traffic
- Utilized Link Analyst, WireShark, and Network Instruments Observer to create graphical LAN/WAN mappings and solve LAN/WAN network problems
- Conducted impact analysis of architectural and engineering designs for enterprise systems
- Administered network solutions to support NAS/SAN storage using vendors, such as EMC
- Worked with stakeholders to prepare and present briefings to military customers, facilitating needed information

**SAIC,** O'FALLON, IL October 2000-October 2003

**TRAINING DEVELOPMENT SPECIALIST II/CISCO NETWORKING ACADEMY INSTRUCTOR**

- Provided Cisco Networking Academy Programming instruction (training) to U.S. Air Force personnel
- Maintained lab network as System/Network Administrator
- Taught Internetworking courses, including Basic and Advanced Routing and Switching, Cisco Network Design, and Network Security
- Configured and performed IOS upgrades for extensive selection of Cisco routers, switches NAS and SAN.
- Reviewed, tested, and evaluated IT systems and IT infrastructure ensuring the alignment with organizational goals and standards
- Evaluated and tested the design and implementation of security controls

**U.S. ARMY RESERVES,** MULTIPLE LOCATIONS, U.S. June 1992-October 2018

**COMMANDER, LOGISTICS/INFORMATION ASSURANCE/S6/IAM/TRANSPORTATION OFFICER**

- Primary responsibilities include leadership, strategic planning, cross-functional teaming, collective training, and accountability for all personnel and resources.
- Developed and implemented IA policies, procedures, and workforce structure to maintain secure environment.
- Managed large-scale projects and programs, developing and verifying resource allocation, benchmarking, funding, and deliverables.