Guy T. Teets, GICSP, GSTRT
Clermont, FL 34711

863-216-9221 | guy.t.teets@gmail.com
https://www.linkedin.com/in/guyteets/ |Portfolio: https://DataVakt.net/

CYBER-PHYSICAL SYSTEMS & INFRASTRUCTURE SECURITY LEADER

Technology Strategy & Innovation Leader

Mission-driven technology leader with a proven record of impact across defense, themed entertainment, and critical infrastructure. Skilled at building and leading high-performing teams to solve complex challenges in wireless, cybersecurity, and enterprise network systems—delivering secure, resilient solutions aligned with regulatory, security, operational, and human needs. Known for bridging the gap between engineering precision and strategic vision, leading with integrity, curiosity, and a deep respect for the people in front of and behind the systems.

SELECTED MAJOR PROJECTS

- **Epic Universe Parkwide Wireless Deployment (Universal Creative):**
  Directed the design, installation, and activation of Wi-Fi 6, DAS, two-way radio, and emergency responder systems across a 750+ acre theme park resort. Led RF spectrum coordination and wireless system compliance from construction through test & adjust.

- **Rise of the Resistance & Millennium Falcon (Disney):**
  Led vulnerability discovery and mitigation efforts for complex OT/ICS ride systems. Acted as field SME for the Fluidmesh (now Cisco CURWB) wireless mesh network during system test & adjust at Walt Disney World and Disneyland.

- **Guardians of the Galaxy & Tiana's Bayou Adventure (Disney):**
  Designed OT security architecture, including Layer 1–3 segmentation, firewall rulesets, and log aggregation integration. Co-authored the AOT Security Policy Standard (AOTSPS), adopted across future Walt Disney Imagineering attractions.

- **JRSS & MPLS 10G/100G Upgrade (DISA – NES/CSRA):**
  Delivered TSIPs, BOMs, and readiness packages for 27 global DISA facilities. Created a time-zone coordination workflow that cut field delays by 50% and reduced deployment durations by up to 10 days across PACOM, EUCOM, and CENTCOM.

EXPERIENCE

Universal Creative – Universal Destinations & Experiences, Orlando, FL   2023-Present
Engineering and Safety | Parkwide Systems Manager Ride & Show Engineering

Directed the Parkwide Systems team's wireless systems strategy and implementation for Universal's Epic Universe, a 750+ acre theme park campus including 3 new resort hotels and extensive back-of-house support facilities. Led full lifecycle infrastructure for Wi-Fi, cellular DAS, LoRaWAN, BLE, and temporary communications—from design, test & adjust, through delivery to the theme park and hotel operations teams. Managed 4 direct reports and 6 vendor partners to ensure seamless integration of wireless systems supporting guest experience, safety, and construction readiness.

- Engineered and deployed redundant MiMosa and Peplink-based networks for construction-phase testing, life safety systems, and 24/7 security communications.
- Coordinated RF spectrum usage and FCC licensing across Wi-Fi, DAS, LoRaWAN, BLE, and Motorola two-way systems, mitigating interference and ensuring regulatory compliance.
- Led infrastructure QA, vendor coordination, and field testing to resolve deployment issues and ensure

readiness across guest-facing and operational environments.
- Oversaw vendor design reviews, scopes of work, FATs, and SATs for multimillion-dollar wireless packages, ensuring compliance with specifications, creative intent, and milestone delivery.
- Delivered stakeholder briefings and turnover documentation supporting readiness across Hotel Operations, Park Operations, Security, and UPT Wireless Engineering.

The Walt Disney Company, Walt Disney World, Orlando, FL **2018-2023**
Sr. Cybersecurity Systems Specialist, Operational Technology Cybersecurity (OTC) Sr. Systems Project Engineer, Operational Technology Cybersecurity (OTC) Systems Technical Specialist, Attractions Wireless Technology

Led cybersecurity strategy and integration within Global Engineering & Technology (GE&T), securing industrial control systems (ICS) and operational technology (OT) networks for new and legacy attractions across Walt Disney World. Directed security architecture, network segmentation, SCADA/PLC hardening, firewall integration, and threat mitigation for ride and show control systems. Oversaw cybersecurity design reviews, coordinated vulnerability discovery and remediation, and acted as the on-site SME during system commissioning and test & adjust. Integrated cybersecurity controls into wireless, hybrid OT/IT, and embedded environments—aligning with the Purdue Model, Zero Trust principles, and Disney enterprise security policy.

- Co-authored the AOT Security Policy Standard (AOT-SPS), a Disney-approved cybersecurity framework that adapted Purdue Model principles for attraction environments by merging OT levels 0/1 and 2/3.
- Designed and implemented OT network segmentation, firewall controls, and centralized logging for major attractions, including Guardians of the Galaxy and Tiana's Bayou Adventure, integrating PLC and embedded system hardening.
- Led vulnerability discovery, automated scanning workflows, and mitigation efforts for Rise of the Resistance, Millennium Falcon, and Guardians—accelerating remediation timelines and ensuring compliance with policy and audit requirements.
- Acted as the on-site SME during testing & adjusting and commissioning phases, supporting wireless system integration across Wi-Fi, Bluetooth, RFID, and Fluidmesh (now Cisco CURWB).
- Reviewed Layer 1–3 OT network and cabling designs to ensure compliance with AOT-SPS standards and secure infrastructure implementation across attractions.
- Delivered executive briefings, risk tracking documentation, and audit-ready reports aligned to attraction construction milestones in coordination with WDI, Engineering Services, and Enterprise Technology.

NES / CSRA - Defense Information Systems Agency (DISA) – Global Support **2014-2018**
Lead Design Engineer, Network Systems MPLS and JRSS Site Survey & Installation (Contract) (remote)

Managed a fully remote 17-person engineering team supporting DISA's Joint Regional Security Stack (JRSS) and MPLS 10G/100G modernization initiatives. Led on-site field surveys at high-priority global locations while overseeing survey and installation teams across CONUS, CENTCOM, EUCOM, and PACOM regions. Directed the development of technical packages and infrastructure readiness plans, serving as primary liaison between DISA stakeholders, cybersecurity engineers, and installation teams to ensure scalable, compliant, and secure network upgrades.

- Led implementation of 27 JRSS and MPLS 10G/100G upgrade projects across 15 countries and 11 U.S. states, deploying 75+ mission-ready network nodes with 95%+ on-time, within-budget delivery.
- Developed complete Telecommunications Site Installation Packages (TSIPs) including BOMs, rack elevations, redline drawings, cable schedules, and Layer 1/2/3 network diagrams in Visio.
- Designed a global coordination workflow to eliminate time zone delays between field teams in UAE, Italy, and Japan—cutting response times by 50% and reducing deployment durations by up to 10 days.

- Validated site infrastructure for compliance with DoD standards—assessing fiber routes, AC/DC power loads, HVAC provisioning, rack integrity, and grounding continuity.
- Mentored junior engineers on site survey protocol, QA/QC documentation, SD-WAN readiness, and protocol configurations (BGP, OSPF, QoS) to ensure engineering accuracy across remote teams.
- Delivered executive briefings and ITP/IT&A milestone reports to DISA and partner agencies, communicating risk posture, installation progress, and SLA-aligned deployment forecasts.

Lockheed Martin - GSM-O (DISA Contract), Global Support   **2013-2014**
Senior Network Systems Support Technician (remote)

Executed field engineering tasks in support of DISA's Global Information Grid (GIG), performing installation, upgrade, troubleshooting, and validation of secure network systems across CONUS sites. Deployed on 4-hour notice to resolve outages and assist with mission-critical cutovers, coordinating directly with DISA's Network Operations Center (NOC), base personnel, and long-haul carriers. Provided Tier III hands-on technical support and contributed to QA documentation to ensure compliance with DISA installation standards and operational continuity.

- Deployed across CONUS on 4-hour notice to troubleshoot outages, validate encrypted VPN circuits, and execute critical network cutovers for classified DISA communications infrastructure.
- Installed and configured IP routers, switches, PROMINA multiplexers, TACLANE encryptors, and secure fiber-optic cabling, supporting circuit activation and handoff to DISA NOC.
- Performed AC/DC power validation, grounding compliance, and fiber testing using OTDR to prepare Layer 1 infrastructure for equipment commissioning and live traffic routing.
- Utilized oscilloscopes, RF test equipment, and packet tracing techniques to verify signal integrity, diagnose transmission faults, and validate protocol performance (BGP, OSPF, VLAN).
- Produced rack elevations, BOMs, cable run lists, and Visio-based redline drawings to support TSIP documentation and QA/QC audit readiness.
- Coordinated directly with Tier III NOC teams and field partners to execute ITP/IT&A procedures, validate network configurations, and close out site tickets within SLA windows.

ADDITIONAL RELEVANT EXPERIENCE

Network Systems Implementer Level II

Logistics Analyst Level II

MILITARY EXPERIENCE

U.S. Navy (13+ Years)
Cryptologic Technician Maintenance | Logistics Specialist | Electronic Warfare Technician

EDUCATION & CERTIFICATION

- **Bachelor of Science (B.S.), Cybersecurity Management & Policy**, University of Maryland Global Campus
- **Associates in Arts (A.A.), General Education**, University of Maryland University College

Certifications

GIAC (Global Information Assurance Certification)
- **[GSTRT (Strategic Planning, Policy, and Leadership)](), GIAC – Issued 2023**
- **[GICSP (Industrial Cybersecurity Professional)](), GIAC – Issued 2023**