accumentum PATHPROOF

TS/SCI W/ FULL SCOPE POLY · ISSE · RMF · VULNERABILITY MANAGEMENT · CONTINUOUS MONITORING



Chari Pollard

// Information Systems Security Engineer · Security Authorization · System Hardening · Risk Analysis

Multi-skilled cybersecurity professional in information systems security engineering, risk management, continuous monitoring, vulnerability remediation, and mission-critical operational support. Active TS/SCI with Full Scope Polygraph. Holder-asserted CAP, CEH, CHFI, SecurityX, Security+, and Network+.

TS/SCI w/ Full Scope Poly | CAP · CEH · CHFI | CASP · Security+ · Network+ | RMF / POA&M / Continuous Monitoring | Windows · VMware · Cisco · Active Directory

LOCATION	Fort Meade, MD
OPENNESS	Open to roles
PATHLOCK	Not connected
STATUS	Best aligned for information systems security engineering, ISSO/ISSE, RMF, continuous monitoring, system hardening, and mission-critical cybersecurity support roles
CLEARANCE	Active TS/SCI with Full Scope Polygraph
FOCUS	Security authorization, POA&M tracking, risk analysis, vulnerability remediation, secure configuration validation, and technical security guidance
CORE STACK	Windows Server, VMware, Active Directory, DNS, DHCP, Remedy, Nessus, SCCM, firewalls, VPN, Cisco infrastructure, and enterprise audit tooling
PUBLIC PROFILE	pathproof.accumentum.net/p/chari-pollard

01 By the Numbers

20+

Years of Technical Security Experience

Career history spans enterprise Windows administration, information assurance, system hardening, vulnerability management, RMF, and secure support operations.

300+

Controls Reviewed & Self-Tested

Completed extensive control validation and self-testing across authorization and reauthorization efforts to sustain agency and NIST alignment.

4

System Security Plans Supported

Maintained compliance, patch accountability, and supporting documentation across multiple active system security plans.

2

Graduate Degrees Completed

Earned advanced degrees in Cyber Technology and Cloud Computing Systems, reinforcing security engineering and modern infrastructure depth.

02 Highlights

ISSE · SLA SUPPORT · SECURITY AUTHORIZATION

Supports Monthly Security & SLA Readiness

Provides technical support to help agency systems meet monthly service level requirements while supporting A&A efforts, RMF activities, secure system validation, and security reporting across classified and unclassified environments.

SLA Support · A&A · NIST 800-53 · IATT / ATO

RMF · CONTINUOUS MONITORING · VULNERABILITY REMEDIATION

Executed 300+ Control Self-Tests

Performed security self-testing across more than 300 controls during authorization and reauthorization efforts, using Nessus and baseline review processes to drive system-level remediation and stronger compliance posture.

300+ Controls · Nessus · Baseline Review · Continuous Monitoring

DOD SECURITY POSTURE · AUDIT REVIEW · POA&M TRACKING

Managed Security Documentation End-to-End

Supported system security plans, continuous monitoring, audit review, decommissioning, risk assessments, vulnerability tracking, and POA&M lifecycle management while coordinating with system owners and stakeholders.

SSP · POA&M · Risk Assessments · Audit Reviews

SYSTEMS ADMINISTRATION · DEPLOYMENT SUPPORT · SECURE INFRASTRUCTURE

Built Security from the Server Layer Up

Delivered hands-on administration across Windows Server, VMware, DNS, DHCP, VPN, wireless, patching, and virtual infrastructure while supporting NIPR, SIPR, and other mission environments requiring hardened, always-available systems.

Windows Server · VMware · DNS / DHCP · NIPR / SIPR

03 Experience

AT&T · INFORMATION SECURITY ENGINEERING · AGENCY COMPLIANCE — Jan 2021 — Present

Information Systems Security Engineer

- Provides technical support to ensure agency systems meet monthly SLA requirements and remain aligned with security expectations.
- Supports Authorization and Accreditation efforts using NIST 800-53 RMF across the design lifecycle for classified and unclassified systems.
- Reviews risk and security assessment reports and provides recommendations to support reauthorization activities.
- Configures and validates secure systems and physical controls and tests security products to detect weaknesses.
- Assists ISSOs with waivers, liens, information gathering, compliance monitoring, vulnerability scanning coordination, and system self-test validation.
- Provides technical guidance for security incidents, reporting activities, and integrated security system support.

AITECH · ISSO / ISSE · RMF EXECUTION

Oct 2019 — Dec 2021

Information Systems Security Officer / ISSE (Level 1)

- Served as security technical advisor for full system security testing to ensure agency and NIST policy enforcement.
- Acted as liaison between administrators, engineers, and authorizing stakeholders to help deploy new technologies and complete QRC efforts.
- Made recommendations using RMF guidance under NIST SP 800-30 and 800-39.
- Completed self-testing reports across more than 300 security controls during authorization and reauthorization efforts.
- Conducted Nessus scans, interpreted results, and recommended baseline fixes to administrators and engineers.
- Reviewed OS settings, monitored security requirements, and supported continuous monitoring across mission-critical platforms.

JACOBS ENGINEERING · DOD CONTINUOUS MONITORING · SECURITY DOCUMENTATION

Apr 2016 — Oct 2019

Information Systems Security Officer

- Supported DoD information system security posture through RMF continuous monitoring activities.
- Performed daily, weekly, and monthly reviews to sustain system compliance and audit collection management.
- Conducted decommissioning activities and created System Security Plans using DoD in-house tools.
- Performed risk assessments in accordance with RMF and NIST SP 800-30 / 800-39 guidance.
- Tracked vulnerabilities, IAVAs, patches, and POA&Ms through mitigation and risk acceptance.
- Worked with stakeholders to maintain current system security documentation, access controls, and system responsibilities.

LEIDOS · SYSTEMS & NETWORK ADMINISTRATION · SECURITY PLANNING

Feb 2013 — Apr 2016

Systems and Network Administrator

- Provided security planning, assessment, risk analysis, and risk management for secure infrastructure systems.
- Supported DNS, email, VPN, wireless networks, firewalls, and enterprise authentication through troubleshooting and maintenance.
- Performed system audits to assess security issues, mitigate findings, and report results.
- Maintained virtual machines, DNS, DHCP, and implementation support for multiple IT systems.
- Ensured systems were operated, maintained, and disposed of in accordance with internal security plans and practices.
- Supported four active system security plans and tracked patches for compliance using agency tooling.

DSCI · NETWORK OPERATION CENTER, CAMP PHOENIX, KABUL, AFGHANISTAN · DEPLOYED IT SECURITY SUPPORT · AFGHANISTAN

Mar 2012 — Dec 2012

IT Security Specialist / System Administrator

- Provided enterprise-level administration and engineering support across Windows Server, SAN, and desktop systems in NIPR, SIPR, and Centrix networks.
- Worked with ISSE teams to conduct weekly security and vulnerability scans across multiple networks.
- Helped enforce government policies protecting confidentiality, integrity, and availability of information systems.
- Supported preventive maintenance and secure operation of complex datacenter virtual environments using VMware vSphere and ESXi.
- Implemented security patches using SCCM and scanning tools in alignment with IAVA and other defense guidance.

Continued · pathproof-chari-pollard

TECH USA INC. · GLOBAL ENTERPRISE COMMAND CENTER, NATIONAL SECURITY AGENCY, FORT MEADE, MD · ENTERPRISE MONITORING · PATCH COMPLIANCE

Jul 2009 — Mar 2012

Windows System Administrator

- Monitored, diagnosed, troubleshot, and escalated issues on Windows Server environments supporting global warfighter operations.
- Processed agency-approved IAVA patches for Microsoft and RHEL/Linux systems and tested releases before deployment.
- Maintained 100% functional systems through enterprise monitoring tools and updated antivirus definitions across managed environments.
- Tracked issues through Service Manager and maintained standard operating procedures as needed.
- Applied incident response knowledge to develop, manage, and administer procedures and scripts for system response activities.

L-3 STRATIS · V44 RAPID RESPONSE CENTER, NATIONAL SECURITY AGENCY, FORT MEADE, MD · ACTIVE DIRECTORY · RAPID RESPONSE OPERATIONS

Jan 2005 — Apr 2009

Windows System Administrator

- Managed Active Directory environments including Group Policy, server and file access, and user account lifecycle administration.
- Monitored and diagnosed system performance using enterprise monitoring platforms to ensure continuous functionality.
- Worked with ISSOs to validate privileged access and keep authorizations current.
- Supported system owners by enforcing malware protection and ensuring incidents were reported according to NSA/CSS policy.
- Developed standard operating procedures, coordinated corrective actions, and escalated complex issues to senior management when needed.

04 Credentials & Qualifications

Vendor certifications are holder-asserted unless a live issuer check succeeded

CLEARANCE

TS/SCI with Full Scope Polygraph

Trusted to support highly sensitive environments that require disciplined security engineering, rigorous compliance, and mission-ready operational reliability.

SECURITY CERTIFICATIONS

CAP, CEH, CHFI, CASP, Security+, Network+

Certification portfolio reflects depth in authorization, ethical hacking, forensics, advanced security practice, and core network and security fundamentals.

MICROSOFT & INFRASTRUCTURE

MCSE, MCSA, MCP, Check Point CCSA

Strong systems foundation across Microsoft enterprise administration, network operations, firewall administration, and secure infrastructure support.

SECURITY DISCIPLINE

RMF, Continuous Monitoring, POA&M, Risk Assessment

Hands-on experience with secure system validation, risk assessment and impact analysis, vulnerability administration, and security authorization lifecycle support.

CAP · ISC2	Holder-asserted
CEH · EC-Council	Holder-asserted
CHFI · EC-Council	Holder-asserted

SecurityX · CompTIA — Holder-asserted

Security+ · CompTIA — Holder-asserted

Network+ · CompTIA — Holder-asserted

05 Technical Skills

// SECURITY ENGINEERING

- Risk Management Framework (RMF) — Core · 96
- Continuous Monitoring — Advanced · 93
- POA&M / Security Authorization — Advanced · 92
- Risk Assessment & Impact Analysis — Strong · 90

// VULNERABILITY & HARDENING

- Vulnerability Scanning — Core · 94
- System Hardening — Advanced · 91
- IAVA / Patch Management — Advanced · 90
- Audit Review & Control Validation — Strong · 88

// SYSTEMS & INFRASTRUCTURE

- Windows Server / Active Directory — Core · 95
- DNS / DHCP / Remote Desktop — Advanced · 90
- VMware / Virtualization — Strong · 88
- Firewalls / VPN / Network Security — Strong · 87

// PLATFORMS & TOOLS

- Cisco Infrastructure — Strong · 86
- Remedy / Service Manager — Advanced · 89
- SCCM / Security Scan Tooling — Strong · 87
- Technical Documentation — Core · 92

06 Let's Put Chari To Work

Best aligned for information systems security engineering, ISSO/ISSE, RMF execution, continuous monitoring, vulnerability management, system hardening, enterprise Windows administration, and mission-critical cybersecurity roles in highly secure environments.

07 Education

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Master of Cyber Technology

Graduate education completed in June 2024, reinforcing advanced capability in modern cybersecurity strategy, systems protection, and technical security leadership.

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Master of Cloud Computing Systems

Graduate study completed in September 2025, supporting secure cloud-oriented thinking across infrastructure, systems design, and enterprise technology modernization.

DEVRY UNIVERSITY

Bachelor of Science in Technical Management

Foundational academic training in technical management complements extensive real-world experience in system administration, security operations, and compliance execution.

PROFESSIONAL DEVELOPMENT

Security, Microsoft & Infrastructure Certification Portfolio

Professional development spans advanced security certifications, Microsoft enterprise credentials, Check Point administration, and network security training aligned to high-trust operational environments.

PathPay funds the path. PathPass gets you through the exam. PathLock keeps the letters. PathProof shows the work.

Accumentum confirms the training and practical work completed with us. Certifications are listed by the professional, and many can be checked with the issuing organization in one click.

pathproof-chari-pollard.pdf · Holder-asserted vendor certifications · Not Pathlock, Inc. · Not a staffing firm · No employment guarantee.

Accumentum® · 12600 Hill Country Blvd Suite 5200 · Austin TX 78738