accumentum PATHPROOF

RMF · ASSESSMENT & AUTHORIZATION · NIST SP 800-53 · DOD/FEDRAMP · ZERO TRUST



Amandeep Singh

// Senior Cybersecurity SME · CISSP, CISM, CASP+, PMP · RMF & A&A Leader

Cybersecurity leader focused on Risk Management Framework authorization, security architecture, and risk reduction across DoD, federal, and enterprise environments. Experience spans Assessment and Authorization, NIST SP 800-53, FedRAMP, and DISA STIG programs. Holder-asserted CISSP, CISM, SecurityX, PMP, and Security+.

CISSP | CISM | CASP+ | PMP | Security+ | RMF & A&A | NIST SP 800-53

LOCATION	Fort Belvoir, VA
OPENNESS	Open to roles
PATHLOCK	Not connected
STATUS	Best aligned for RMF authorization, security architecture, A&A, and federal cybersecurity leadership roles
FOCUS	RMF, cybersecurity architecture, vulnerability management, Assessment & Authorization, NIST SP 800-53 / STIG compliance
CURRENT	Senior Cyber Security Analyst · MindPoint Group · December 2021 – Present
PUBLIC PROFILE	pathproof.accumentum.net/p/amandeep-singh

01 By the Numbers

CISSP
Headline Credentials
CISSP, CISM, CASP+, and PMP are listed in the professional headline, with CISM, CompTIA Advanced Security Practitioner (CASP), and Security+ among certifications.

RMF
Authorization Leadership
Principal-level leadership of NIST SP 800-37 RMF lifecycles, FedRAMP alignment, DISA STIG enforcement, and continuous-monitoring programs.

A&A
Assessment & Authorization
Hands-on validation of controls against live environments—configuration analysis, firewall/ACL review, routing tables, scan data, logs, and architecture diagrams.

6
Organizations
MindPoint Group, SAIC, AnaVation LLC, Kforce Inc, Secure Innovation, and DELTA Resources, Inc.

02 Highlights

MINDPOINT GROUP · SENIOR CYBER SECURITY ANALYST

NIST 800-53A Control Assessment

Conducts security control assessment using NIST 800-53A guidance for information technology systems and cloud solutions, develops and updates security authorization packages in accordance with FISMA, and presents findings to intelligence and acquisition community audiences.

NIST 800-53A · FISMA · Authorization Packages · Risk Assessment

SAIC · DEPARTMENT OF STATE ISSM

FedRAMP Migration & Xacta 360

Served as principal cybersecurity advisor to the Department of State's ISSM. Led migration of security control implementations to updated FedRAMP requirements and operated Xacta 360 as the system of record for GRC, evidence artifacts, and POA&M tracking.

FedRAMP · Xacta 360 · DoS ISSM · POA&M

ANAVATION LLC · FORT BELVOIR, VA

Army Night Vision & AI Imaging

Engineered iterative security test and re-test methodologies for Army Night Vision and Electronic Sensor Systems and provided security engineering support for an AI-enabled imaging platform built on a Hadoop environment.

Army NVESS · AI/ML Hardening · Hadoop · Accreditation

KFORCE / SECURE INNOVATION · QUANTICO, VA

NCIS A&A and Navy Validation

Managed the full A&A lifecycle for multiple NCIS information systems in eMASS and Xacta as a Navy Qualified Validator, and executed RMF and DIACAP A&A across DoD and Navy environments using eMASS, Xacta, and MCCAST.

eMASS · Navy Qualified Validator · DIACAP-to-RMF · NCIS

03 Experience

MINDPOINT GROUP · CONTROL ASSESSMENT · AUTHORIZATION PACKAGES — Dec 2021 — Present

Senior Cyber Security Analyst

- Conduct security control assessment using NIST 800-53A guidance for various Information Technology systems and Cloud Solutions.
- Develop and update security authorization packages in accordance with FISMA and the client's requirements.
- Monitor, identify and report security risks within the Group's information technology domain. Perform regular risk assessments and monitoring to enforce clients' security policies and procedures, reducing the overall security risks of the IT assets.
- Present security findings to various intelligence and acquisition community audiences to increase awareness of security risks and the implementation of security controls.
- Assist with quarterly assessments of testing, control effectiveness, residual risk, and risk metrics and encourage proactive identification of weaknesses and/or control gaps, while providing sound recommendations to address control gaps.

Continued · pathproof-amandeep-singh

SAIC · SCA · DEPARTMENT OF STATE ISSM — Jun 2020 — Dec 2021

Senior Cyber Security Engineer / Security Control Assessor

- Served as principal cybersecurity advisor to the Department of State's ISSM, partnering with system owners, engineers, and program offices to assess and accredit information systems supporting U.S. foreign policy missions through rigorous NIST SP 800-53A control assessments and risk-based recommendations.
- Led the migration of security control implementations and authorization documentation to align with updated FedRAMP requirements; mapped existing controls to revised baselines, identified inheritance opportunities from authorized CSPs, and delivered remediation roadmaps that closed gaps without disrupting operations.
- Operated Xacta 360 as the system of record for GRC activities—centralizing control libraries, evidence artifacts, and POA&M tracking; streamlined the A&A workflow and produced reporting that gave senior leadership clear visibility into the authorization portfolio and residual risk posture.
- Authored comprehensive FedRAMP documentation including System Security Plans (SSPs), policies, and procedures aligned to the NIST SP 800-53 control catalog; collaborated with CSPs to clarify shared responsibility boundaries, resolve technology gaps, and harden the enterprise defensive posture.
- Conducted detailed risk assessments and security impact analyses across the SDLC; quantified residual risk to confidentiality, integrity, and availability and provided strategic security guidance to senior leadership during FISMA audit cycles and authorization renewals.

ANAVATION LLC · FORT BELVOIR, VA · INFORMATION ASSURANCE · FORT BELVOIR, VA — Jan 2020 — Jun 2020

Information Assurance Security Specialist

- Engineered iterative security test and re-test methodologies for Army Night Vision and Electronic Sensor Systems; aligned control validation to system CONOPS, exercised controls against operational use cases, and documented evidence sufficient to support accreditation decisions for fielded systems.
- Provided security engineering support to ISSMs and ISSEs accrediting an AI-enabled imaging platform built on a Hadoop environment; assessed control implementations across the data pipeline, evaluated cluster hardening against authentication, encryption, and access governance requirements, and contributed to secure deployment in Army operational environments.
- Developed custom hardening baselines for emerging AI/ML technologies where no formal DISA STIG existed—cross-referencing NIST SP 800-53 controls, CIS Benchmarks, and vendor security guidance to define configuration standards that engineering teams adopted across the program.
- Facilitated assessment-only accreditation of software toolsets supporting Army field deployments, validating that each release met Information Assurance requirements and produced evidence aligned to Army certification authorities.

KFORCE INC · QUANTICO, VA · ISSE · NAVY QUALIFIED VALIDATOR · QUANTICO, VA — Jun 2019 — Dec 2019

Sr. Information System Security Engineer (ISSE) / Navy Qualified Validator

- Managed the full A&A lifecycle for multiple NCIS information systems in eMASS and Xacta; prepared and maintained authorization packages from initial categorization through accreditation and continuous monitoring while coordinating with system owners on POA&M remediation and ongoing risk acceptance decisions.
- Performed Security Control Assessor (SCA) and Information System Security Engineer (ISSE) functions; developed and executed security test plans, validated NIST SP 800-53 control implementations against DoD and Navy IA requirements, and produced Security Assessment Reports documenting residual risk for command authorities.
- Engineered defensive security solutions for NCIS information systems operating in classified environments—integrating controls and countermeasures aligned to mission needs for identity, network segmentation, and data protection across the enclave.
- Led DIACAP-to-RMF transition efforts on multiple inherited authorization packages; reconciled DIACAP IA controls to NIST SP 800-53 control families, rebuilt authorization documentation to meet DoD 8510.01 expectations, and maintained a defensible security posture throughout the migration.

SECURE INNOVATION · QUANTICO, VA · ISSE · QUANTICO, VA

Feb 2019 — Jul 2019

Sr. Information System Security Engineer

- Executed end-to-end RMF and DIACAP A&A lifecycle management across DoD and Navy environments; drove systems to Authority to Operate (ATO) using eMASS, Xacta, and MCCAST in compliance with DoD 8500.01 and applicable NIST publications, tracking authorization artifacts to defensible baselines.
- Conducted comprehensive vulnerability assessments and compliance scans across classified IT environments using Tenable Security Center and ACAS/Nessus; analyzed scan output to distinguish exploitable findings from informational noise, produced detailed risk reporting for system owners, and drove targeted remediation aligned to operational priorities.
- Led PCI-DSS compliance audits and merchant system scoping assessments; defined the cardholder data environment (CDE) boundary, mapped controls to PCI-DSS requirements, and delivered remediation recommendations to system owners ahead of formal QSA review.

DELTA RESOURCES, INC. · WASHINGTON, DC · IT SPECIALIST · WASHINGTON, DC

Jan 2015 — Feb 2019

IT Specialist / Cyber Security Engineer

- Partnered with NAVSEA ISSEs to develop strategic plans that accelerated RMF Assessment and Authorization timelines; identified package gaps early, sequenced control implementations against authorization deadlines, and kept multi-system portfolios on track.
- Reviewed critical A&A package artifacts including Security Plans (SP), SAPs, and Risk Assessment Reports (RARs); validated control narratives against actual implementations, ensured artifact consistency across the package, and confirmed readiness before submission to the Navy Authorizing Official (NAO).
- Performed vulnerability and risk analysis using Endpoint Security Suite (ESS/HBSS) and ACAS/Nessus; correlated findings across host and network scans to characterize the security health of accredited information systems and surfaced systemic issues that single-tool views often missed.
- Coordinated with system points of contact to implement mitigation strategies and update authorization plans; tracked POA&M closure progress, ensured residual risk remained within accepted thresholds, and maintained the security and operational health of naval networks and applications.

04 Credentials & Qualifications

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

GOVERNANCE

Certified Information Security Manager (CISM)

Listed among certifications and in the professional headline alongside CISSP, CASP+, and PMP.

ADVANCED SECURITY

CompTIA Advanced Security Practitioner (CASP / CASP+)

CompTIA Advanced Security Practitioner (CASP) appears in certifications; CASP+ appears in the headline.

FOUNDATIONAL

Security+

Security+ is listed among certifications. Accumentum CompTIA SecurityX training is dated June 2026.

HEADLINE CREDENTIALS

CISSP · CISM · CASP+ · PMP

Senior Cybersecurity SME headline: CISSP, CISM, CASP+, PMP | RMF & A&A Leader | NIST SP 800-53 | DoD/FedRAMP.

CISSP · ISC2 — Holder-asserted

CISM · ISACA — Holder-asserted

SecurityX · CompTIA	Holder-asserted
PMP · PMI	Holder-asserted
Security+ · CompTIA	Holder-asserted

05 Technical Skills

// TOP SKILLS

RMF Assessment & Authorization	Top skill · 92
POA&M Management	Top skill · 90
Vulnerability Analysis	Top skill · 88

// CORE STRENGTHS

Risk Management Framework (RMF)	Core · 91
Cybersecurity Architecture	Core · 89
Vulnerability Management	Core · 90
Assessment & Authorization (A&A)	Core · 98
NIST SP 800-53 / STIG Compliance	Core · 95

// ENVIRONMENTS

FedRAMP alignment	Practice · 76
DISA STIG enforcement	Practice · 74
Zero Trust segmentation	Practice · 72
Shipboard and satellite-connected systems	Practice · 73

// TOOLING NAMED IN ROLES

Xacta 360 / Xacta	Named · 68
eMASS / MCCAST	Named · 69
Tenable Security Center / ACAS/Nessus	Named · 66
ESS/HBSS	Named · 76

06 Let's Put Amandeep To Work

Best aligned for RMF authorization, security architecture, A&A, and federal cybersecurity roles. Contact via LinkedIn only.

07 Education

NORTHERN VIRGINIA COMMUNITY COLLEGE

Associate's degree, CyberSecurity A.A.S

Northern Virginia Community College · CyberSecurity A.A.S.

ACCUMENTUM®

CompTIA SecurityX

Computer and Information Systems Security / Information Assurance · June 2026 – June 2026.

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-amandeep-singh.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