Jose D Soto

954-804-7118 | jds@ph7.us | linkedin.com/in/jose-s-279b3a9a | www.jds-bio.com
U.S. Citizen | U.S. Army Veteran

IT Infrastructure and Cybersecurity Leader | Former CTO and Director of IT

Summary

Technology and security leader with over 15 years in IT and more than 11 years running technology organizations as Manager, Director, and CTO across government, legal, distribution, and managed services. Currently runs infrastructure operations and operational security for the DC Office of the Chief Financial Officer: a roughly $10 million budget, 33 direct reports, and about 1,800 users under NIST 800-53 and IRS Publication 1075. First year results were $2.8 million out of the budget and critical audit findings down more than 40 percent. Before that, moved a 29 office law firm to cloud first infrastructure, built a managed services firm to 30+ clients and a sale, and ran a $5 million IT budget for a two-state distributor for seven years. U.S. Army Signal Corps veteran and published practitioner on NIST 800-53, RMF, and FedRAMP who briefs executives in plain language.

Career Highlights

- Cut $2.8 million from the DC OCFO infrastructure budget in year one while adding capacity: $1.5 million in operating expenses and $1.3 million in capital expenditure.
- Reduced critical audit findings by more than 40 percent through ITGC evidence and root cause remediation in the annual external financial statement audit.
- Moved a 29 office law firm to cloud first infrastructure and cut unplanned downtime roughly in half.
- Built a managed services firm to 30+ client accounts as CTO and co-founder and carried it through to a sale.
- Designed and ran enterprise networks end to end: Arista spine and leaf fabric, BGP multihomed data centers, and certificate based 802.1x access control with Cisco ISE.

Core Competencies

IT and security strategy, roadmaps, and governance | Infrastructure operations to SLAs and KPIs | Cybersecurity operations: SIEM, EDR, threat detection, incident response, root cause analysis | Cloud and hybrid platforms: Azure, Microsoft 365, AWS, GCP, OCI | Compliance and GRC: NIST 800-53, IRS Publication 1075, SOC 2 readiness, ITGC and audit remediation | Zero trust and identity: Entra ID, MFA, conditional access, certificate based 802.1x, NAC | Network architecture: BGP, OSPF, spine and leaf fabrics, SD-WAN, segmentation, wireless | Data center and virtualization | Disaster recovery and business continuity | AI governance and development | Budget and vendor governance, $1 million to $10 million+ | Leadership, mentoring, and teaching

Professional Experience

Office of the Chief Financial Officer, Government of the District of Columbia | Washington, DC
IT Manager, Infrastructure Services Group | 10/2025-Present

- Reduced operating expenses by $1.5 million and capital expenditure by $1.3 million in the first year by reviewing contracts, consolidating redundant tools, right-sizing cloud resources, and adopting newer tools with modern features at lower cost, while expanding overall infrastructure capability.
- Cut critical audit findings by more than 40 percent by supplying ITGC evidence for access, change, and operations in the annual external financial statement audit and remediating findings at the root cause.
- Own a roughly $10 million infrastructure budget and lead 33 direct reports across systems, network, cloud, and platform operations supporting about 1,800 users and devices in cloud, colocation, and on premise environments; senior escalation point for complex issues through root cause analysis.
- Lead operational security across the environment: zero trust roadmap, CrowdStrike endpoint detection and response selection and rollout, and GRC controls managed in Vanta against NIST 800-53 and IRS Publication 1075.
- Direct Azure and Microsoft 365 security configuration for an IRS 1075 aligned tenant build, with Entra ID identity, Microsoft Defender, MFA and conditional access, and certificate based 802.1x network access control (Cisco ISE) across roughly 1,700 endpoints, with compliance logging to Splunk.

- Lead network architecture modernization, including a BGP multihomed design across primary and colocation data center sites, dark fiber route evaluation between facilities, and DNS failover architecture guidance (Cisco Umbrella).
- Run patching, change, and lifecycle management across server, network, and endpoint estates; lead legacy remediation migrating services from shared government platforms to OCFO owned infrastructure and cloud.
- Vet AI enabled platforms for security, privacy, and responsible use, including an AI powered mainframe modernization proof of concept with regulated tax data in scope.
- Manage vendor contracts and evaluations, including EDR procurement, a ThousandEyes network visibility proof of concept briefed to executives, and backup contract stewardship (Cohesity NetBackup) with GASB 96 cost allocation; report roadmap, risk, and investment recommendations to the CIO and executive leadership.

ADVNTBLANKET Corporation | Miami, FL
Chief Technology Officer and Co-Founder | 04/2024-10/2025

- Co-founded an IT services firm and directed infrastructure, security, and service operations across a portfolio of 30+ client accounts spanning sports, entertainment, legal, medical, and electrical infrastructure, through to the sale of the company in 2025.
- Standardized service delivery on HaloITSM, HaloPSA, and HaloCRM with documented policies and procedures, so every engagement ran on consistent, repeatable, compliant operations.
- Established security and compliance standards for managed service delivery and performed risk assessments with Onspring GRC across client environments spanning Azure, GCP, AWS, and on premise networks.
- Acted as principal advisor and escalation point for client engagements, scoping solutions, leading implementations, and managing client IT budgets; strategic IT advisor to the European American Transatlantic Chamber of Commerce.
- Led AI driven application development on Node.js, Supabase, and the OpenAI and Anthropic APIs.

The LaBovick Law Group | Palm Beach Gardens, FL
Director of Information Technology | 09/2022-06/2024

- Ran IT and security for a 29 office firm across Florida and Massachusetts in direct partnership with C-suite leadership; standardized company wide IT policies and security protocols, reducing operational risk.
- Moved the firm to cloud first infrastructure, cutting unplanned downtime roughly in half while modernizing virtualization, storage, and endpoint platforms (Hyper-V, Docker, NinjaOne, Entra ID, Intune, AWS).
- Engineered multi site networking with SD-WAN, site to site VPN, and segmentation; oversaw datacenter hardware and integrated access control systems.
- Deployed Salesforce Litify and built the firm's Moodle Learning Management System for internal and client education; automated the firm's proprietary PIP Practices software with SQL and .NET supporting lead and intake management workflows.
- Raised digital fluency and cybersecurity awareness across 120 staff through hands on training programs.

J.J. Taylor Distributing, Inc. | Jupiter, FL
IT Manager | 06/2015-09/2022

- Owned a $5 million annual IT budget and technology strategy in direct collaboration with the CIO and CFO, supporting 24/7 high availability beverage distribution operations across two states.
- Ran the security stack end to end: CrowdStrike EDR, Microsoft Sentinel, Microsoft Defender, Proofpoint, Mimecast, Sophos, Rubrik backup, and LogRhythm SIEM, with unified endpoint management through NinjaOne, Intune, Entra ID Hybrid, and Workspace ONE across Apple, Android, Windows, and IoT devices.
- Administered ITSM platforms (ConnectWise, Kaseya, ManageEngine) under the ITIL v4 framework, improving incident, problem, and change management across all sites.
- Architected multi site infrastructure on VMware, Windows Server, and Azure hybrid cloud, with enterprise server, storage, and hyperconverged platforms (Dell PowerEdge, HP ProLiant, Fibre Channel).
- Deployed and operated an Arista spine and leaf data center fabric and managed enterprise firewalls and networking across Cisco, Palo Alto, Aruba, and SonicWall, with SD-WAN, advanced site to site routing, and Infoblox automation.

- Oversaw warehouse automation systems and robotics platforms, integrating them with access control and secure connectivity between distribution centers; managed large scale APC power protection at all sites, including warehouse environments.
- Developed, documented, and tested disaster recovery policies enabling rapid business continuity; supervised IT staff supporting local and remote sites and led major upgrade rollouts.

U.S. Army, III Corps | Fort Cavazos, TX
Nodal Network Systems Operator-Maintainer (25N), Signal Corps | 04/2010-12/2014

- Deployed and maintained secure, encrypted tactical communications (WIN-T, satellite, microwave radio, VoIP) for mission critical operations under demanding conditions.
- Installed and terminated fiber optic and copper cabling; operated OSPF routed secure networks and Cisco VoIP platforms; maintained generators and high and low voltage electrical systems sustaining 24/7 field operations.
- Trained junior personnel on secure network deployment, equipment maintenance, and field best practices.

Teaching, Mentoring, and Speaking

- Teaches and mentors at every level, from new hires and junior engineers to peers and senior leadership, turning complex technical and security material into practical guidance.
- Presents at legal conferences and mastermind groups on technology, security, and infrastructure; publishes practitioner guides on NIST 800-53, RMF, FedRAMP, and NIST 800-171 (jds-bio.com).
- Delivers security awareness and technical training across professional and military settings; mentors transitioning service members and fellow veterans entering IT and cybersecurity careers.

Technical Skills

Security Operations: CrowdStrike EDR, Microsoft Sentinel, Microsoft Defender, LogRhythm SIEM, Splunk, Huntress, Bitdefender, Proofpoint, Mimecast, Sophos, Vanta GRC, Onspring

Identity and Access: Entra ID, Microsoft Intune, MFA and conditional access, Cisco ISE 802.1x, internal CA certificates, zero trust

Cloud and Hybrid: Microsoft Azure, Microsoft 365, AWS, GCP, Oracle OCI, hybrid identity and tenant security

Network: Cisco (Catalyst, ISE, Umbrella), Palo Alto, Aruba, Arista (spine and leaf), SonicWall, Ubiquiti, Juniper, BGP, OSPF, SD-WAN, VPN, DNS and DHCP, Infoblox, ThousandEyes

Data Center and Virtualization: VMware vSphere, Hyper-V, Nutanix, KVM, Docker, Dell PowerEdge, HP ProLiant, Fibre Channel, APC power systems

Platforms and Automation: NinjaOne RMM, HaloITSM, HaloPSA, HaloCRM, ConnectWise, Kaseya, ManageEngine, Rubrik, Cohesity NetBackup, Synology, PowerShell, SQL, .NET, Node.js, OpenAI and Anthropic APIs

Education

M.S., Management, Emphasis in Information Systems and Services | University of Maryland Global Campus, 2021 (Graduated with Honors, GPA 3.8)

B.S., Computer Networking and Security, Minor in Business Management | University of Maryland Global Campus, 2018

Additional Training

Network Administrator Program, New Horizons | VMware IT Academy, Caldwell Community College and Technical Institute | U.S. Army Signal Academy, Honor Graduate | DEI in the Workplace Certificate, University of South Florida

Certifications

Oracle OCI Certified Foundations Associate (2025) | CompTIA Network+ | CompTIA A+ | RingCentral Contact Center Admin | ETA Network Systems Technician