



OUT-OF-BAND (OOB)

BATTLECARD: FEDERAL NETWORKS

SELLING NORTH STAR

Lantronix doesn't just make console servers — we sell secure operational continuity for networks that can't go dark. Federal buyers are measured on cybersecurity, compliance, and mission assurance, so every conversation starts there. Our OOB solutions is a TAA-compliant, dedicated, always-available management plane that follows NSA and CISA guidance, satisfies auditors with tamper-evident logs, and keeps agencies in control of critical infrastructure even when the production network is compromised or unreachable.



THE PITCH | Maintain secure control of critical network infrastructure — even when the production network is unavailable. Lantronix out-of-band solutions are built to support Zero Trust initiatives, simplify compliance, and reduce recovery time across distributed federal environments.

Spotting Opportunities for Out-of-Band in Fed

UPTIME

24x7, global operations are common in civilian and DoD networks. Whether it's citizen services or military operations, uptime is critical and the network needs to work as designed.

SECURITY

Federal networks are prime targets, and OOB is part of the cybersecurity posture. Both NSA and CISA have published guidelines recommending OOB to segment management traffic from operational traffic.

COMPLIANCE

Federal network guidelines are thoroughly spelled out and tracked. Lantronix OOB solutions satisfy security and audit requirements across agencies with logging, authentication, encryption, centralized audit.

NEW OPPORTUNITY DRIVERS

Federal buying season is late summer/early fall. Start discussions early to allow time for proof-of-concept testing and purchasing.

Enterprise network expansions, refreshes, and upgrades.

Increasing security compliance, access, and reporting requirements.

Multi-site operations needing 24/7 monitoring, automated responses, and alerts.

SLC 9000 — BUILT FOR FEDERAL PRIORITIES

Supports Zero Trust network access policies | TPM 2.0, encrypted storage, secure granular access; every action authorized and accountable.

Isolated management plane | Dedicated OOB path with integrated 4G/5G cellular + eSIM, independent of production paths.

Audit-ready logging | All sessions logged with a tamper-evident audit trail.

Automation for small teams | OpenAPI 3.01 REST API, ZTP, and Ansible integration.

Availability by design | Dual power (AC or DC), dual Ethernet failover, tested cellular failover.

Objection Handling

OBJECTION	RESPONSE
We already have VPN access.	VPN depends on the production network. OOB access remains available when that network is down or misconfigured.
We rarely use console ports	When you do (think outages, failed upgrades, security incidents) it's mission critical.
It's another device to manage.	Centralized management, automation, and ZTP reduce admin effort while adding a resilient recovery path.
Our network is already secure.	Security lowers incident probability. OOB reduces impact when failures or cyber events still occur.
We don't have budget.	Weigh platform cost against truck rolls, downtime, & mission disruption. One avoided outage can offset much of the investment.

One OOB Architecture, Right-Sized: Lead with the SLC 9000

Lead with the SLC 9000 for data centers and large sites. For branch offices and remote locations needing **8 or fewer console ports**, position the EMG family. The whole fleet is managed through PercepXion with a single audit trail.

	SLC 9000 — LEAD	EMG 8500	EMG 7500
BEST FOR	Data centers, hyperscalers, large distributed sites, new deployments	Branch offices & remote sites where space is limited; modular flexibility	Small & unmanned sites — retail, ATMs, cell towers — where cost and space matter most
MANAGED PORTS	Up to 48 in 1RU (RJ45, USB, Ethernet) in 16-port increments	Up to 8 via field-replaceable modules (RJ45 serial, USB, or Ethernet)	Up to 8 (RS-232 / USB), fixed configuration
CONNECTIVITY	Integrated 4G/5G + eSIM; dual GbE + dual 1-10GbE SFP+	4G/LTE cellular, Wi-Fi, or dial-up OOB options; dual GbE or SFP fiber	Integrated LTE cellular with failover/failback
SECURITY & COMPLIANCE	TPM 2.0, 128GB encrypted storage, tamper-evident session logs, TACACS+/RADIUS/LDAP	FIPS 140-2 crypto (Cert #2398), NDAA compliant, TACACS+/RADIUS/LDAP	FIPS 140-2 crypto (Cert #2398), NDAA compliant, TACACS+/RADIUS/LDAP
MANAGEMENT	PercepXion SaaS + full OpenAPI 3.01 REST API, ZTP, auto-discovery	PercepXion SaaS — single pane of glass, ZTP	PercepXion SaaS — single pane of glass, ZTP

What Federal Buyers Care About

PAIN	WHAT THEY'RE THINKING	YOUR ANGLE
Locked out of a router	“How do I recover this remotely?”	Hardware-level console access via a dedicated OOB path
Production network failed	“I still need a way in.”	Integrated cellular stays up independent of production paths
Staffing shortages	“I can't send admins onsite to deploy OOB.”	ZTP + PercepXion: deploy and manage sites without sending network admins
Cyber attack	“Can I still manage infrastructure?”	Segmented management plane per NSA/CISA OOB guidance
Audit findings	“Can I prove who accessed what?”	Tamper-evident session logs, centralized in PercepXion
Large distributed environments	“One way to manage thousands of devices.”	Single pane of glass + full REST API for fleet automation

NEVER FORGET: Risk reduction, compliance, lifecycle support, and mission assurance outweigh feature comparisons. Every purchase is viewed through a cybersecurity lens.

TALK TRACK: “Standardize on one out-of-band architecture: SLC 9000 in the data center and larger sites, EMG at the branch and edge, all under PercepXion with one inventory, one policy engine, and one audit trail across every site.”

QUALIFYING QUESTIONS TO ASK

- “How do you provision new console servers today — how many people, how long does it take?”
- “Does your team run Ansible, Terraform, or ServiceNow?”
- “When something breaks at a remote site, what does recovery look like?”
- “What did your last audit say about access logging on network gear?”
- “What’s kept you from doing more with OOB — setup complexity?”