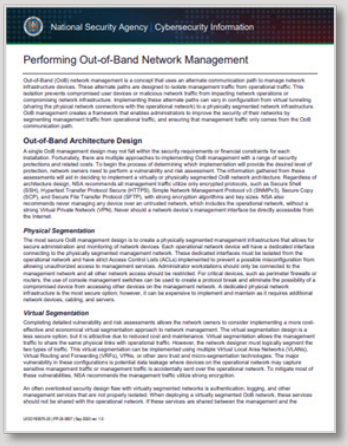
LANTRONIX®

LANTRONIX Out-of-Band EVERYWHERE

SOLUTION BRIEF

NSA RECOMMENDS OUT-OF-BAND MANAGEMENT FOR GREATER NETWORK CYBERSECURITY

The National Security Agency (NSA) published guidelines for using out-of-band management to create a framework that improves network security by segmenting management traffic from operational traffic. By ensuring that management traffic only comes from the out-of-band communications path, compromised user devices or malicious network traffic is prevented from impacting network operations and compromising network infrastructure.


National Security Agency | Cybersecurity Information

Performing Out-of-Band Network Management

Out-of-Band Architecture Design

Physical Segmentation

Virtual Segmentation

The NSA's recommendation of this type of network architecture reaffirms the Lantronix stance on network management. For over 20 years, we've built a platform for out-of-band network management that increases cybersecurity through isolating management and operational traffic. This architecture also enables reliable automation which makes managing enterprise networks easier and more effective.

Improving Network Infrastructure Cybersecurity: The NSA on Isolating Management Traffic from Operational Traffic

The NSA defines two basic architectures for out-of-band design:

- Virtual Segmentation
- Physical Segmentation

Virtual segmentation can initially be appealing because it utilizes the existing connections to network infrastructure, but isolates management traffic by using multiple VLANs, VPNs or other zero-trust and segmentation technologies. There are a couple of caveats to virtual segmentation:

- Strong encryption must be used to avoid potential data leakage if management traffic is accidentally sent over the operational network.
- Often overlooked is not properly isolating authentication, logging and other management services. If these services are shared between the management and operational network, it could create a hop point between the two that could be exploited.

Physical segmentation is what it sounds like: both the management network and the operational network have a dedicated interface, with separate access controls. The NSA says that a dedicated physical network infrastructure at Layer 1 of the network is the most secure option.

Lantronix deploys in the rack with the network infrastructure and connects over the console port. Management access to devices can be limited to only the serial connection, ensuring that the management network is physically separated from the operational network.

Recommendations

The NSA document includes four recommendations for implementing out-of-band network management.

1. Implement Encryption

The NSA recommends utilizing only encrypted protocols on all out-of-band management traffic, including VPNs when connecting to management networks over and operational network.

Lantronix encrypts all data, whether in motion or at rest. When a network administrator connects to an Lantronix Local Manager over an out-of-band link, a Reverse SSH and/or IPSEC tunnel is established automatically. Multiple users are supported, and network management protocols are re-routed. Network administrators direct changes using the Control Center or SSH to the Local Manager which can use TACACS/RADIUS/Active Directory or just about any 2FA to authenticate and authorize users. Vendor applications can be tunneled to the admin's workstation.

Data stored onsite in the Lantronix Local Manager resides on a 256GB Opal 1.2 NVMe drive capable of 256-bit AES compliant data encryption in FIPS 140 mode. The Lantronix LM-Series secures the whole platform (hardware and software) and as a result puts the entire solution through the rigorous FIPS 140-2 certification process.

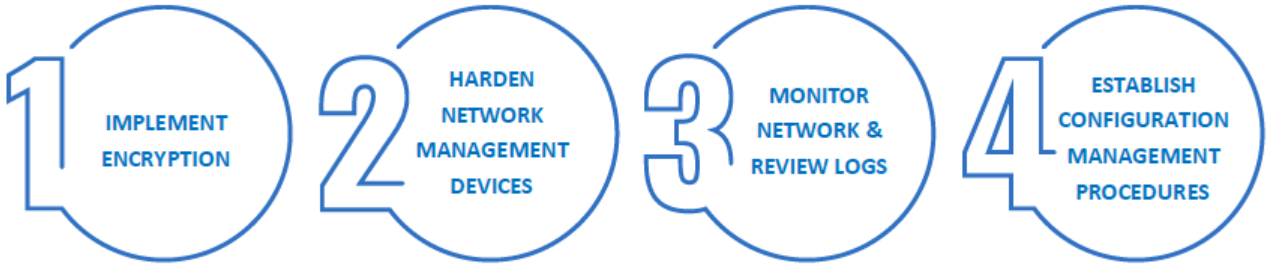
2. Harden Network Management Devices

The NSA recommends using only serial connections for critical devices. This helps reduce running unnecessary services on devices like routers and switches. Lantronix creates the sanctioned management path to devices over the console port. Using dedicated Ethernet connections, Lantronix provides secure management access to servers using IPMI as well as devices like firewalls that need out-of-band access for troubleshooting.

Lantronix is a secure, closed appliance. Unlike console servers with open access to the OS, with Lantronix, the underlying Linux OS is locked down for higher security and reliability. This ensures that non-approved scripts and software cannot be installed, secrets (like passwords and keys) are kept from users, and that the application software and configuration integrity of the management device itself is maintained.

Lantronix integrates with multi-factor authentication for secure device access and the Lantronix Control Center (UCC) allows for the creation of user types to govern not only access to remote sites, but also which devices users can reach, and which commands they can implement. Security protocols are maintained even when the network is down, which is especially important because this is often when traditional management tools go "dark" leading to vulnerabilities.

Access groups are easily managed in the UCC. The Lantronix Control Center can be deployed in a high availability configuration for resiliency.



3. Monitor Network and Review Logs

The NSA recommends monitoring and verifying network connections on a regular basis as well as having a process for checking logs and then actually following that process by defining roles and responsibilities of administrators.

The Lantronix platform has built-in logging that can trigger alerts and/or automated actions based on a number of inputs:

Physical – Has the console connection been unplugged? Did a device reboot? Lantronix is a state-aware console server, any change in state is noticed and recorded. What about power? Lantronix integrates with a managed power distribution unit as well. Lantronix monitors input from network Layers 1-3 on a continual basis. Collecting device data over the console port ensures a supply of information that's not dependent on the network, can be collected more frequently than centralized NSM tools, and is more detailed and parsed locally to drive actions. Beyond device data, from its position onsite in the rack with network infrastructure, Lantronix conducts service level tests of the network itself to add performance and trending data to the alerting, decision, and automation process.

Access – Who has logged into a device and what did they do? Lantronix logs every session and keystroke for maximum accountability. Logs are saved locally and backed up on the UCC for long term use.

NSA says to monitor and verify network configurations on a regular basis. Lantronix has built-in automation that can verify managed devices are running the expected OS and configurations and then alert or push the standards to devices automatically. This really leads into the next topic:

4. Establish Configuration Management Procedures

Lantronix' ability to act as a gateway for secure out-of-band access, continuous monitoring, and automated actions really comes together around config management. Whether it's watching for changes to devices on the network, recording management activity from users or saving configs and OS files locally to reduce response times when there are issues, Lantronix has unique capabilities for config management. In fact, Lantronix holds the patent on network management over the console port.

Unlike other solutions with scripting environments that are both difficult to manage and secure, Lantronix comes ready to deploy with built-in routines that ensure configuration management is standardized, limiting opportunities for human error.

A built-in rules engine makes it possible to create custom rules without coding that can be shared across the deployment to take advantage of data gathered from monitoring over the console port.

Lantronix can automate standardizing OS on network devices. Users can upload and define a standard OS image for a given managed device make and model in the Lantronix Control Center to create an OS policy. When defined for a group in the UCC inventory tree, this policy will automatically download the standard OS image for a given make and model from the UCC to all Local Manager device ports in that inventory group and in its subgroups that match the make and model. It is stored as a named OS with the name "standard." If a managed device does not match the standard OS defined in the policy, Lantronix can alert or push the standard OS to the device.

Summary

When it comes to isolating network management traffic from operational traffic, Lantronix is really built for the task. That explains why we've deployed in highly secure networks in the federal space, both civilian and DoD, as well as financial, healthcare and more.

Combining out-of-band access with local storage, processing and network management software establishes a separate management plane for network infrastructure. Add to that the Lantronix Control Center for archiving and user controls across an enterprise deployment, and you have a proven platform for improving cybersecurity with true out-of-band network management.

© 2026 Lantronix, Inc. All rights reserved. Lantronix is a registered trademark of Lantronix, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners. Specifications subject to change without notice. 032426

LANTRONIX®