# Deployment of Palo Alto Firewalls to Secure GDOT's Edge Network

By Georgia Department of Transportation
5/29/2025

## Benefits Statement

To safeguard Georgia's expansive transportation network, Georgia Department of Transportation (GDOT) is deploying advanced firewalled routers statewide, protecting 8,000+ connected devices from growing cybersecurity threats. By integrating secure edge devices into traffic systems, GDOT reduces the risk of cyberattacks that could disrupt safety-critical operations like signals and ramp meters. Standardized installation procedures and cross-team coordination streamline deployment, saving time and ensuring consistent configurations. This proactive approach protects both infrastructure and public safety, while reducing future costs linked to system breaches, downtime, and emergency responses.

## In this case study you will learn:

1. How cybersecurity risks increase as communications infrastructure grows, especially from IoT devices at network edges like traffic signals and cameras.
2. How GDOT utilized the PA-450 firewall device to secure both fiber and cellular communications, addressing both technical and security needs statewide.
3. How cross-department teams developed uniform installation procedures, streamlining device deployment and strengthening long-term network resilience.

2025
TSMO Award
Winner
for
Cybersecurity and TSMO
NOCoE

**Project #206**

**Version Number: 1**

## BACKGROUND

GDOT’s SigOps and ITS focused teams have worked closely with the Department’s IT experts over the past few decades to deploy one of the nation’s largest remote transportation communications networks along Georgia arterial and interstate roadways. This network now covers approximately 8,000 remote communications devices supporting traffic signals, ramp meters, cameras, dynamic message signs, remote weather information systems, roadside unit, etc. Along with these remote communications devices comes concerns of physical and virtual cyber-security.

In addition to upgrading its physical security for ITS infrastructure, GDOT has recognized the need to protect its virtual network from growing cyber-security risks presented by edge network end points. Continually advancing IoT devices within the transportation sector present great potential safety and operational benefits, but also create new risks to State DOTs. Each new device connected at the edge of a network, such as at a traffic signal cabinet, present the potential for a new security threat. Connections pose a risk not only to the individual edge device but also to the entire agency network.

When the time came to plan for life cycle replacements of remote communications devices, GDOT’s Office of Information Technology recommended TSMO staff pursue routers and switches which incorporate firewalls at the edge. After evaluating market leaders, Palo Alto Networks’ PA-450 device was selected to support both cellular and fiber communications statewide. This was the only device available which was designed specifically as a firewall which also met GDOT’s needs for multiple communications methods, port availability, field hardening, Power over Ethernet (PoE), etc. Over the next five years, GDOT is confident it will be ready for ever increasing cyber-security threats, especially as it relates to major event planning and management.

## TSMO PLANNING, STRATEGIES AND DEPLOYMENT

This process involved collaboration with GDOT’s TSMO and IT teams including staff focused on arterial and interstate operations, field device maintenance, communications design, and network management. As existing field communications devices were reaching the end of the software and security support periods, these teams collaborated to identify technical requirements for it's next generation of devices, to be deployed over five years as individual devices reached end of life. Requirements and considerations included communications types, available number of ports, field hardening, PoE availability, network management features, form factor, and cost.

The overall product evaluation and selection process went smoothly because of multiple TSMO strategies which have been integrated within GDOT. GDOT's robust arterial and interstate operations programs focus on regional and statewide deployments which it can deploy, manage, and maintain. These programmatic practices have led to the development of Department SMEs in operations, maintenance, communications design, and network management. TSMO strategies both provided the opportunity to rely on these experts as well as ensured each had a hand in selecting devices that meet operational, cybersecurity, and maintenance needs both for the present and future.

## COMMUNICATIONS PLANNING AND EXECUTION

Planning and execution for this project involved experts throughout the Department. Teams included operations and communications staff focused on functional needs, maintenance staff focused on technical device needs, information technology staff focused on cyber-security and network management needs. These teams maintain on-going relationships through day-to-day program practices. When the need was identified, these teams worked seamlessly to outline a shared list of requirements and arrange meeting with vendors and manufactures to jointly evaluate products.

While collaboration for this project is limited to within GDOT, the impacts to external agencies will be significant over the next 5 years. In building a statewide TSMO program over the past two decades, GDOT has established on-going relationships with over 100 local cities, counties, CIDs, and other partners. These relationships have allowed GDOT to collaborate with local agencies to develop mutually beneficial infrastructure and practices.

Additionally, these relationships allowed GDOT's experts to evaluate devices with local agency concerns in mind such as ease of network management, contract availability, and ease of installation for technicians.

## OUTCOME, BENEFITS AND LEARNINGS

While this project is still within the early stage of deployment, several outcomes have been achieved. Multiple subject matter experts worked together to select a security focused firewall which also meets other technical and functional needs. These teams worked together to arrange for selection of a primary device, power supplies, antennas, and mounting accessories which will address contextual needs for locations across the state.

Additionally, GDOT worked early on to develop procedures and guidelines for installation of SIM cards, one-touch provisioning, uniform configuration and standard installation of these devices. The development of these processes and documents provides for an efficient transfer of devices between multiple teams. Overall deployment time is significantly shortened by these practices and individual teams are able to better anticipate receipt of new devices from partners elsewhere in the Department.