Port of Los Angeles
Cybersecurity Services Proposal – Los Angeles Port Police
Sole Source Justification

Activity

The Port of Los Angeles (POLA) has requested a proposal to provide a cybersecurity solution to The Los Angeles Port Police mission-critical systems to ensure long-term cybersecurity safety and success. By enabling 24x7 monitoring capabilities within the Los Angeles Port Police mission-critical environments, POLA will be provided with deeper visibility and the ability to proactively detect cybersecurity threats to the Los Angeles Port Police public safety network. These mission-critical environments include the Motorola ASTRO® Radio Network Infrastructure, the Motorola Computer-Aided Dispatch (CAD), and the Motorola Records Management System (RMS).

Vendor will Provide

Motorola is providing a market leading Managed Detection and Response (MDR) solution for each of the Los Angeles Port Police networks (ASTRO®, PremierOne CAD, PremierOne RMS) with Motorola's SOAR platform, known as ActiveEye. This solution provides connectivity to our geographically redundant Security Operations Centers (SOC) operating 24 hours a day, 7 days per week, 365 days per year. Motorola will be able to notify the Port of Los Angeles of active threats and the activities used to detect/investigate possible threats through threat hunting services. Motorola will also provide Cybersecurity Advisory services to achieve a lower risk profile and increased cyber resilience.

Justification for Noncompetitive Contract

At Motorola Solutions, we understand the complexity and critical nature of our ASTRO® Radio, CAD and RMS systems, and the importance of providing cyber security services while maintaining the best system availability and performance levels.

The ActiveEye MDR solution leverages our advanced ActiveEye security platform and experienced analysts to detect and respond to cyber threats in your Motorola environment, in addition to the Enterprise IT environment. All systems are monitored under a single pane of glass providing efficient monitoring capabilities with full visibility to the security status of our partners' networks and systems. In 2023, the Los Angeles Police Department (LAPD) purchased the ActiveEye security platform to help protect their PremierOne CAD and RMS. Taking into consideration that the Los Angeles Port Police system is a tenant on the Los Angeles Police Department's CAD and RMS shared system, contracting with Motorola for CAD and RMS MDR coverage will allow for full coverage across the shared system, as well as coordination of alerts by utilizing the same solution between agencies.

Motorola Solutions' Security Operations Center (SOC) team works independently from, but collaborates closely, with the product teams to address any potential findings that may impact your systems. Having direct access to ASTRO® and PremierOne specialized engineers, who are intimately familiar with the Port's public safety networks, allow our SOC team to provide precise results and guidance on how to mitigate threats.

The ActiveEye MDR solution is the only MDR platform approved by Motorola Solutions for deployment into the ASTRO® radio network to protect the system from Cybersecurity threats without potentially jeopardizing the integrity and reliability of the network. Other Cybersecurity

Solutions have not been tested on ASTRO® and would invalidate the support agreements for adding non-certified integrations.

ASTRO® radio systems are highly engineered and tested to ensure mission-critical levels of availability and performance. Maintaining this performance requires that only trusted and certified integrations are present in the system. In order to provide critical managed support services such as Tech Support, Dispatch, and Network Monitoring, it is vital that the system does not contain non-certified integrations. For this reason, Motorola Solutions Managed Services Statements of Work (SOWs) specifically exclude support services in these cases:

- Systems with non-standard configurations that have not been certified by Motorola.
- Solutions' Systems Integration and Test (SIT) team are specifically excluded from this service, unless otherwise agreed in writing by Motorola Solutions.

The ActiveEye MDR service continuously undergoes the highest level of independent testing and certification by the ASTRO® team. These tests include:

- Functional testing to ensure that the security controls work within the ASTRO® network and that they do not interfere with the behavior and functioning of the systems within the network.
- Stability testing to ensure that MDR for ASTRO® does not impact the stability and availability of the ASTRO® network.
- Performance testing to ensure that MDR for ASTRO® does not reduce the level of performance in the ASTRO® network.
- Ongoing patch verification (SUS/RSUS) against all supported releases to ensure that patches do not introduce a regression in functionality or performance.

No other MDR provider has the capability to perform this extensive and rigorous testing of their solution to ensure that network performance and availability are preserved. Motorola now includes MDR for ASTRO® in each software release to ensure future versions also meet the cybersecurity needs of these radio networks.

Cost Benefit Analysis

Entering into a contract with a third-party to implement a similar cybersecurity solution would constitute wasteful spending, as it would fail to capitalize on the established ActiveEye MDR integration already present on the shared CAD/RMS system with the LAPD. Furthermore, implementing this MDR solution within the Los Angeles Port Police ASTRO® system will satisfy the requirements needed for the current support agreement between Motorola and the Los Angeles Port Police. It is unlikely that a third-party solution will provide the Los Angeles Port Police with any greater product than the proposed solution from Motorola, as other parties do not share the required knowledge of the Motorola proprietary networks. Motorola has invested significantly in the collection of people, process, and technology, which has allowed Motorola to take industry standard security controls and adapt them to be able to operate safely and effectively inside a mission-critical network.