



January 13, 2026

To whom it may concern,

In accordance with federal and state security guidelines (specifically Section 889 of the National Defense Authorization Act), we are committed to maintaining a secure and reliable supply chain. Our priority is to protect our infrastructure and our clients' data from vulnerabilities associated with certain foreign-produced technologies.

## Our Sourcing Standards

We certify that we do not procure, use, or provide any equipment, systems, or services from the following prohibited entities or their subsidiaries:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Furthermore, we do not obtain equipment or services from any entity owned, controlled, or directed by "covered foreign countries," which include The People's Republic of China, The Russian Federation, or any state sponsors of terrorism.

## Why This Matters

Modern telecommunications and video surveillance equipment handle vast amounts of sensitive information. By restricting the use of hardware and software from high-risk entities, we mitigate the risk of:

- Cyber-vulnerabilities and unauthorized data access,
- Foreign adversary exploitation of critical infrastructure, and
- Security breaches during the delivery of our services.

We take these regulations seriously. Compliance with these standards ensures that our partnership with all our clients remains secure, transparent, and legally sound. Should you have any questions or require further information, please do not hesitate to reach out.

DocuSigned by:

A handwritten signature in black ink, appearing to read "Matt Ignor".

B231BB11BE9340B...

Matt Ignor, VP Operations  
mignor@miovision.com | 519-574-0444