INFOBRIEF

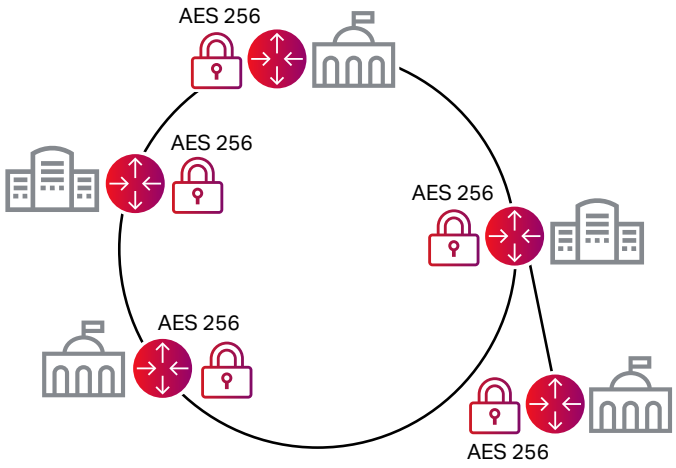
Local Government Encryption

With municipal, county, and state government remaining a high-priority target for hacking, many IT and security teams are looking to strengthen their holistic security capabilities rather than relying purely on perimeter security. This includes ensuring all data is encrypted at rest (for example, when in a storage array) and in flight.

Government agencies at all levels and their contractors involved with any type of Criminal Justice Information (CJI) are required to encrypt both at-rest data and in-flight data. The CJI Services (CJIS) Security Policy requires that when CJI is transmitted outside the boundary of a physically secure location, the data must be immediately protected via encryption. When encryption is employed, the cryptographic module used must be certified according to Federal Information Processing Standards (FIPS) 140-2, and use a symmetric cipher key strength of at least 128 bit.

The CJIS controls apply to contractors, private entities, noncriminal justice agencies, or members of a criminal justice entity with access to, or who operate in support of, criminal justice services and information. The CJIS audit unit conducts information technology security audits to assess agency compliance with the CJIS Security Policy, including whether in-transit data is encrypted according to FIPS.

Ciena provides hardware-based Advanced Encryption Standard (AES) 256-bit encryption with FIPS certification capable of supporting up to 200 Gb/s per card with minimal incremental latency for encryption between data centers and regional headquarters. Ciena's encryption solutions



provide a wide range of benefits to municipal, county, and local governments—including helping with CJIS requirement compliance. In addition, bifurcated management provides separate network and security management that allows IT staff to manage the network while the security team manages the keys. Finally, Ciena's FIPS-certified solution can help protect from both financial and reputational damages caused by data breaches involving the personal information of citizens.

Deploying Ciena's encryption solution does not require government IT departments to conduct a major 'rip and replace' of their current network. Ciena's packet-optical platform with the AES 256-bit encryption card can be deployed strategically within an existing network infrastructure.

Was this content useful? Yes No