USE CASE: U.S. LOCAL COUNTY

CJIS Compliance with FIPS 140-2 Certified Technology

SITUATION ANALYSIS

Approximately two years ago, a leading U.S. local county government ("County") on the east coast failed a CJIS audit and was required to encrypt their data on FIPS 140-2 Certified technology. This County is responsible for and supports over 500 public departments within their jurisdiction, including local schools, libraries, police and fire departments, social services, and others. All of these public departments interoperate and communicate with one another, including transmitting sensitive data over a connected fiber optic network infrastructure.

The County has three major Data Centers, of which one serves as a backup in the event of a network breach or failure. These Data Centers are dispersed but connected using optical fiber. There are two fiber rings that connect the Data Centers and these rings run in diverse paths so that the County can assure 100% availability of all of their network systems should one segment of the Fiber Ring fail.

Of the 500 locations supported by this County and connected to one of multiple Data Centers, less than five percent of policy and fire departments require encryption of their data in accordance with CJIS requirements.

These 23 sites were deemed most critical because they failed their previous audits. These sites need to meet the applicable CJIS requirements and will do so by utilizing FIPS 140-2 certified encryption technology.

CHALLENGE

The County had previously failed a CJIS audit, so it was imperative that they take the action that was required. Certes Networks contacted the County, to assist them with their CJIS compliance.

And, because there were less than ten standalone network systems that need to be FIPS 140-2 Certified, it was determined that it would be best to start encryption technology implementation at the Data Centers and then pick up the remote sites as they were enabled with encryption appliances.

The initial implementation is to deploy four CEP appliances, i.e., CEP520, on the interconnecting links between the two Data Centers. This will allow all data flowing between these two Data Centers to be encrypted and to meet the FIPS 140-2 requirement. The remainder of the network will be completed over a three-year period as the budget permitted.

SOLUTION REQUIREMENTS

Certes Networks has to insert CEP 520's in front of the County's routers at each of the two Data Centers. Once encryption between to the two Data Centers is verified, FIPS 140-2 configuration will be enabled on all four CEP 520s. The Certes support team will work closely with the County security and IT teams to configure and deploy the policies and FIPS140-2 technology.

THE SOLUTION

Certes Networks is able to provide a simple, scalable and uncomplicated encryption solution through their Layer 4 technology, which includes placing Certes Enforcement Point (CEP) appliances between Data Centers. This technology can be employed without having to disrupt, move or replace the County's current network infrastructure.

And, with the Certes key management system software, CryptoFlow® Net Creator (CFNC), the County is able to define and deploy policies to ensure that only data matching those deployed policies will be transmitted between the Data Centers.

RESULT

By implementing the FIPS140-2 validated CEP 520 and CFNC key management system, the County will have a solution that encrypts all of their data in transit between the two Data Centers. Further, the Certes Networks Layer 4 solution is one more step toward meeting the County's compliance objectives for the next audit cycle. The policies and keys deployed will strengthen the County's security posture and their compliance with the CJIS requirements.

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com

We offer an encryption solution that is simple, scalable and uncomplicated.