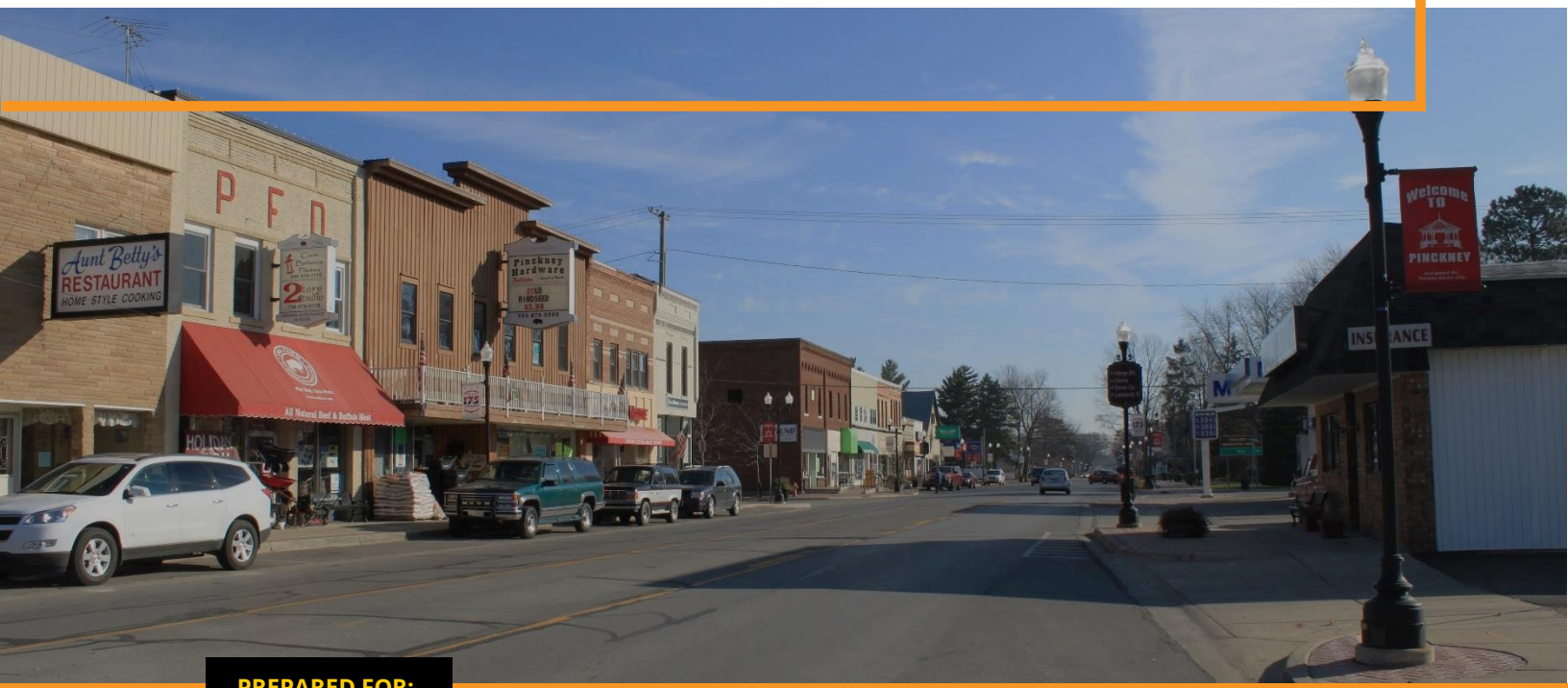
brightlineIT

PROJECT PROPOSAL



PREPARED FOR:

VILLAGE OF PINCKNEY

Village of Pinckney
220 S Howell St.
Pinckney, Michigan 48169
www.villageofpinckney.org

COVER LETTER

IT Committee
Village of Pinckney
220 S Howell St.
Pinckney, MI 48169

Jonathan Williams, Solutions Engineer
Brightline Technologies
10355 Citation Dr
Brighton, MI 48116
248-886-0248

To whom it may concern,

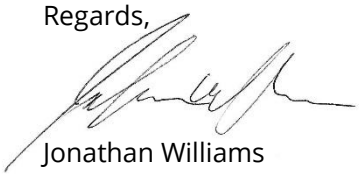
During the course of onboarding, Brightline has assessed the Village's current IT infrastructure and interviewed key stakeholders at the Police Department in order to prepare a set of recommended upgrade projects that meet the Village's requirements for CJIS compliance and modernize the Village's IT posture. Below is a summary of the recommended projects in order of priority:

1. Event Logging
2. Server Upgrade / Network Segmentation
3. Firewall Upgrade
4. WiFi Upgrade

If you or your team have any questions regarding this proposal, you may reach me by phone at 947-207-1142 or by email at jwilliams@brightlineit.com.

Thank you for your time and consideration in reviewing our proposal.

Regards,

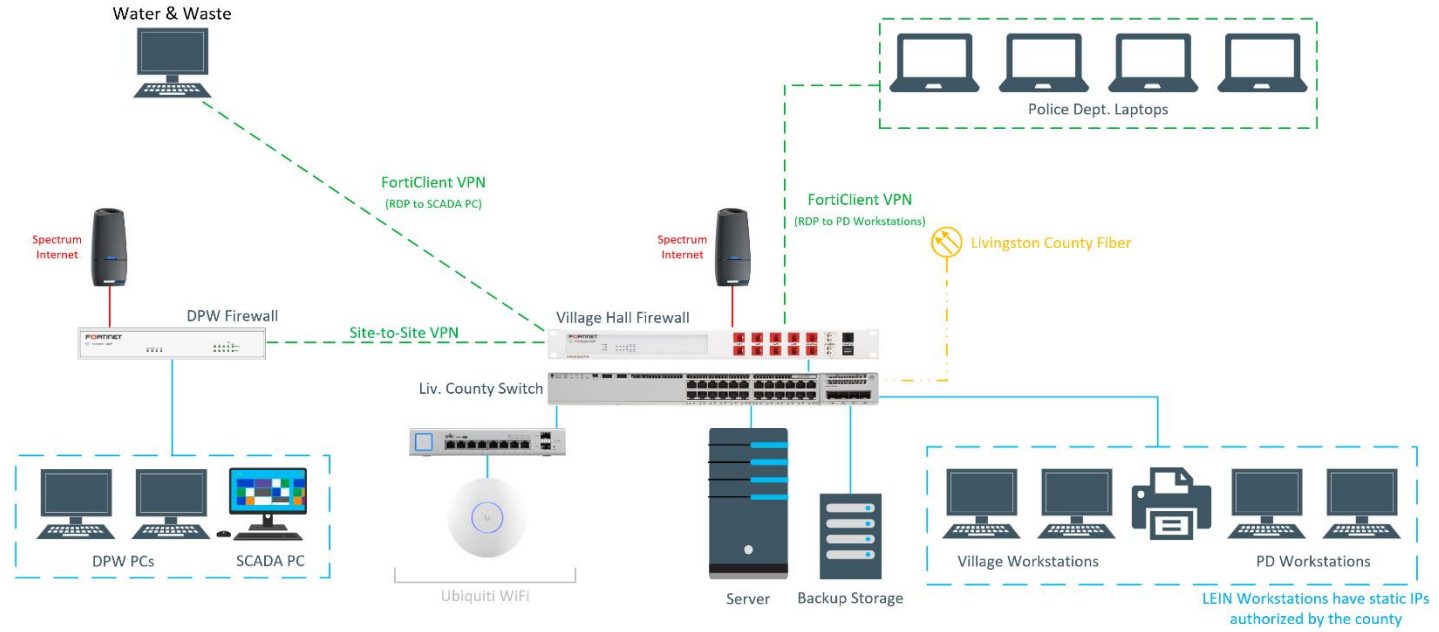


Jonathan Williams
Solutions Engineer, Brightline Technologies

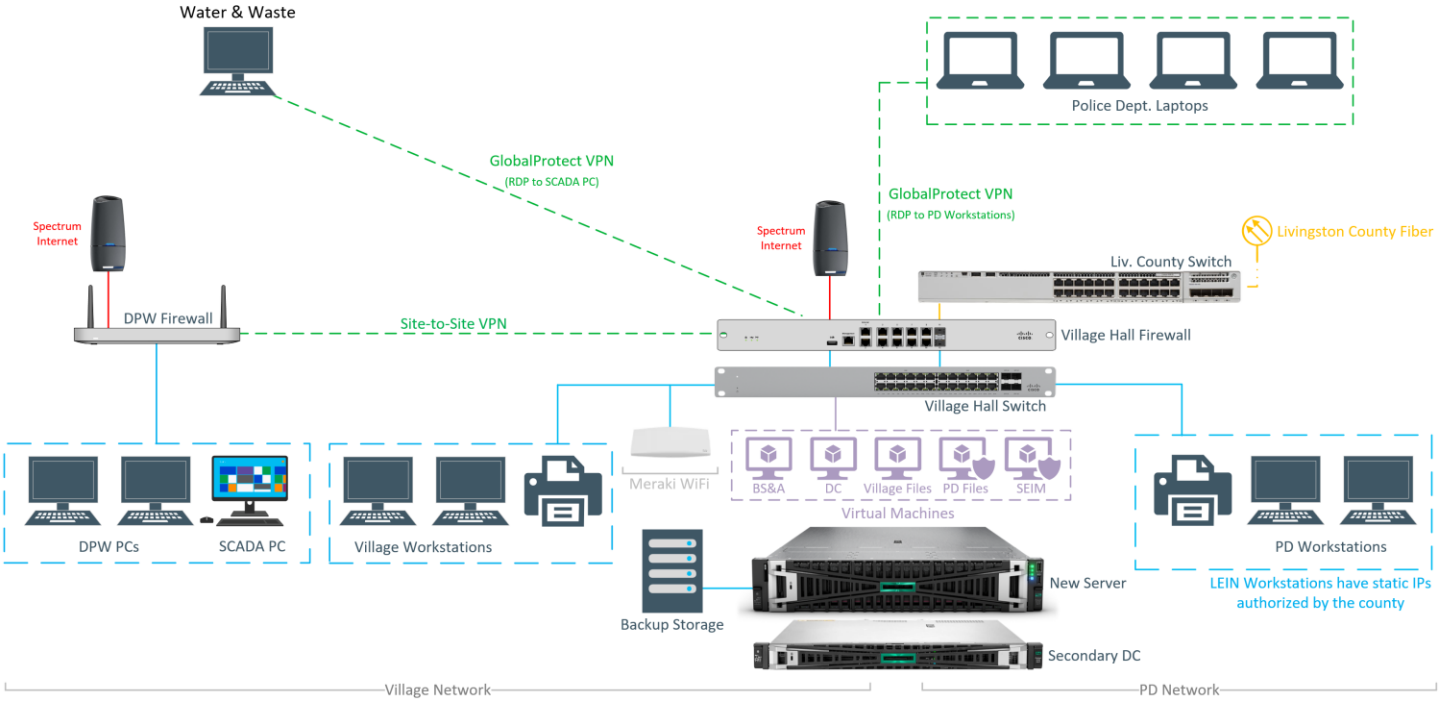
OVERVIEW

Below are infrastructure diagrams of your current environment and our proposed environment. Full resolution versions of these diagrams are provided in the appendices to this proposal. These are "layman's" diagrams intended to provide clarity for the council and should not be used for security audits. As we complete these projects, we will update the LEIN network diagram to match the current network state.

Current Environment



Proposed Environment



PHASE ONE: Event Logging

LEIN REQUIREMENTS

The final missing piece in completing your LEIN audit requirements is to enable event logging for Police Department authentication and file access to the P: drive, which holds CJI. The event logs must be retained for one year (at minimum) to be compliant. Your current server lacks the storage and processing power to maintain the level of logging required by LEIN. This is where a Security Information & Event Manager (SIEM) comes in. A SIEM ingests, storages and categorizes event logs in a central repository for long-term storage, reporting, alerting, and searching. For police departments, this means better awareness of potential threats, suspicious activities, and vulnerabilities within their network. By analyzing this data, a SIEM can ultimately help detect patterns indicative of security threats, including unauthorized access attempts, which is an example of an event required to be captured per the current CJIS Security Policy.

NeQter Compliance Engine

Brightline recommends NeQter to meet the event logging requirements in the short term and improve the Village's overall security posture long-term. NeQter is a plug-and-play SIEM product with built-in dashboards and reports that can be automatically delivered via email at any cadence for easy review. With Event Management at its core, NeQter also includes features to help prepare the Village for future compliance requirements as they work their way down from the Federal and State levels, like Vulnerability Management.

Unpatched vulnerabilities in software are the second-most common breach vector for organizations across the world and is the most common vector for nation-state hackers. NeQter includes vulnerability management features that scans your server, computers, and network infrastructure for open vulnerabilities. Not all vulnerabilities can be fixed by running updates, sometimes configuration changes are required to properly plug the gaps in hardware and software. Brightline will configure the vulnerability scanner to run quarterly and provide reports to the village on recommended remediation and mitigations.

NeQter helps allocate resources effectively by prioritizing security incidents based on severity so the Village can focus their efforts on critical issues rather than sifting through vast amounts of data.

DEPLOYMENT

While NeQter does offer hardware appliances in a variety of configurations, Brightline recommends deploying NeQter as a virtual machine (VM) as it is more cost-effective and allows for easy expansion of resources in the future, if needed. Your current server does not support virtual machines. In Phase Two, we are recommending a server upgrade that includes virtualization. However, that project has a lot of moving pieces and will take several months to procure, configure, and install.

In the meantime, you need to get event logging in place now... more like last year. So, to get that up and running as soon as possible, we can lease you a temporary server to hold the NeQter VM until we get the new server in-place. Once you have a new server, we can easily migrate the NeQter VM to the new server. The NeQter deployment includes configuring it to meet the requirements outlined in the CJIS Security Policy as well as training Chief Garrison on how to use the dashboards, reports and search features of the product.

COST ESTIMATES

Recurring Costs

- Temporary Server Lease - $250/month
- NeQter Subscription - $4,320/year or $10,800/3-year
  *While the 3-year price is significantly cheaper; you essentially get the third year free; it may make more sense for your budget to get the 1-year now and get the 3-year subscription next year.

One-Time Costs

- Server and NeQter Deployment - $4,000
- Windows Server 2022 (2-VM pack) - $1,070
  *This license is transferrable, so we can use it on your new server.

PHASE TWO: New Server / Network Segmentation

CURRENT SERVER

Your current server is a Super Micro physical-only server built by IT Right. Because it is a physical-only server, all server-based functions live and operate together on a single instance of Windows Server: Active Directory, File Services, BS&A, Roadsoft and backup services for the Village and Police Department. Best practice is to separate these functions into separate virtual servers for redundancy, access control and ease of management. Super Micro is a server parts manufacturer that allows organizations to build their own servers on a budget at the expense of support, warranty, and manageability. We recommend sticking to HPE and Dell and maintaining support contracts so that hardware failures can be remediated quickly and with no additional cost.

There are additional compliance steps that cannot be taken while all the Village's services are all running on the same server. For example, we cannot enable encryption-at-rest because the current server does not have a Trusted Platform Module (TPM). A TPM is a hardware chip that manages cryptographic operations on a server or PC. Most PCs and servers manufactured in the last 6 years have a TPM built in. We also cannot enable FIPS mode and encrypt CJI data on the P: drive because BS&A is on the same server as Police data and FIPS mode is known to break SQL-based software like BS&A.

NEW SERVER

We recommend a new server that supports virtualization so we can separate Village data and Police data according to best practices and enable FPIS 140-2 encryption on Police data. Below are the recommended virtual servers to be deployed on the new virtualization server.

- **VOP Domain Controller** – The Village and PD must continue to share an authentication domain due to BS&A's integration with Active Directory.
- **App Server** – This server will host BS&A, Roadsoft and their databases.
- **Village File Server** – This server will host all the Village's file shares like the S: drive and V: drive.
- **PD File Server** – This server will host all Police data, with FIPS 140-2 encryption enabled.
- **NeQter** – The SIEM VM will be migrated from the temporary server to its permanent home on the new server.

Separating the PD files and the Village files will also allow better access control and help to limit the scope of what logs the NeQter needs to ingest, resulting in more relevant data that is more efficient to review. Backup storage will be directly connected to the new server, effectively air-gapping it to further protect backup data in the event of a cybersecurity incident.

SECONDARY DOMAIN CONTROLLER

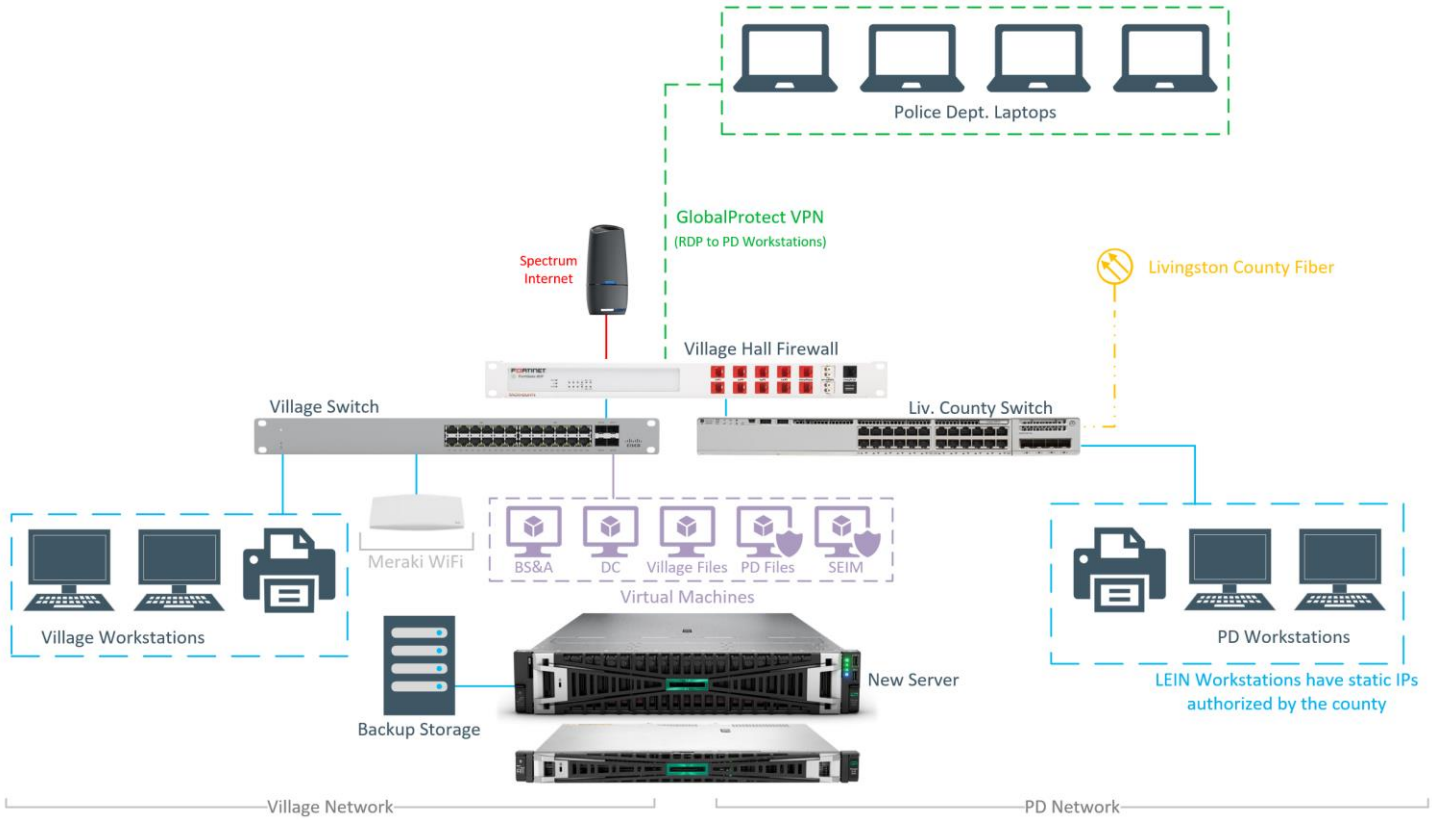
While optional, we also recommend following Microsoft's best practices for Active Directory and having a physical secondary domain controller for fault tolerance and high availability. In an Active Directory domain environment, the domain controllers provide DNS services for the organization, which is a critical service for accessing the internet. If you only have one domain controller, and that domain controller goes offline, users will be unable to log in to their computers and unable to access the internet. With a secondary DC, if one goes down, the other takes over so the Village can continue to operate normally while troubleshooting the issue.

NETWORK SEGMENTATION

To further limit access to CJI on the PD File Server and Livingston County's LEIN system, we recommend segmenting the network at Village Hall, with the Village on one network and PD on a separate network.

Because we do not have access to manage Livingston County's switch, the best way to achieve this without encroaching on the county's turf is with a separate switch. The Police Department will remain on Livingston County's switch and the rest of Village Hall will be on the new switch.

The below diagram illustrates the Village Hall network at the end of Phase Two.



RACK & POWER

In this phase, we will clean up the network closet and consolidate equipment into a ventilated, lockable network rack and add a new battery backup capable of handling the power requirements of the new hardware.

COST ESTIMATES

Recurring Costs

- RMM & Antivirus for new server and virtual servers - $100/month
  **Your agreement includes software four (4) servers. There will be four (4) virtual servers, plus the physical server hosting them and the secondary domain controller for a total of six (6) servers. If you choose not to proceed with the secondary domain controller, the additional monthly will be $50 instead of $100.*
- 3-year Meraki Switch Licensing & Support- $350
  **1 or 5-year licensing available upon request*

One-Time Costs

- New Server - $14,000
- New Network Switch - $2,250
- Rack & Power - $2,000
- Secondary Domain Controller - $3,750 (optional but recommended)
- Microsoft Licensing - $1,000-8,000
  **To finalize the licensing cost, we will need system and database requirements from BS&A. BS&A is currently using SQL Express, which is free. If the database requirements for BS&A continue to support SQL Express, the low end of the price range can be assumed.*
- Deployment & Migration - $15,400

Server Migration Assumptions

- BS&A will migrate BS&A
- MTU will migrate Roadsoft
- Brightline will migrate Active Directory and File Shares

PHASE THREE: Firewall Upgrade

FORTINET & FIPS 140-2

Your current firewalls at Village Hall and DPW are Fortinet FortiGate 80F. Brightline has reviewed the FIPS certificates for Fortinet products and while Fortinet does offer firewall products with FIPS 140-2 validated modules, 80F is not one of validated modules. For that you would need a model ending in 1 (e.g. 81F, 61F, etc). Your Fortinet firewall subscriptions expire on November 24th, 2024. Brightline does not sell Fortinet hardware, software or subscriptions. We recommend moving to a new firewall solution before the expiration date. Preferably, a firewall with a verifiable FIPS certificate.

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date
4614	Fortinet, Inc.	FortiOS 6.2	Firmware	09/27/2023
4613	Fortinet, Inc.	FortiGate-5001E1 Blade with FortiGate-5144C Chassis	Hardware	09/27/2023
4612	Fortinet, Inc.	FortiGate-600D/1200D/1500D/3000D/3700D and FortiGate-5001D with FortiGate-5144C Chassis	Hardware	09/27/2023
4611	Fortinet, Inc.	FortiGate-61E/61F/81E/101E/101F and FortiWiFi-61E	Hardware	09/27/2023
4610	Fortinet, Inc.	FortiGate-3401E/3601E/3960E/3980E	Hardware	09/27/2023
4609	Fortinet, Inc.	FortiGate-201E/301E/401E/501E/601E	Hardware	09/27/2023
4608	Fortinet, Inc.	FortiGate-6300F/6301F/6500F/6501F	Hardware	09/26/2023
4607	Fortinet, Inc.	FortiGate-VM	Software	09/26/2023
4533	Fortinet, Inc.	FortiGate-1101E/2000E/2201E/2500E/3301E	Hardware	06/12/2023
4497	Fortinet, Inc.	FortiGate Next-Generation Firewalls with FortiOS 6.4/7.0	Hardware	05/02/2023
4443	Fortinet, Inc.	FortiOS 6.4/7.0	Firmware	02/23/2023
4415	Fortinet, Inc.	FortiGate-VM 6.4 and 7.0	Software-Hybrid	01/16/2023
4362	Fortinet, Inc.	FortiManager 6.2	Firmware	11/09/2022
4361	Fortinet, Inc.	FortiAnalyzer 6.2	Firmware	11/09/2022
3897	Fortinet, Inc.	FortiWLM-100D and FortiWLM-1000D	Hardware	04/16/2021

CJIS Security Policy

According to the current revision of the CJIS Security Policy, FIPS validated encryption is only required if CJI is being transmitted outside the boundary. Encryption shall not be employed inside the boundary so long as the transmission medium (ethernet) is owned and operated by the Village and the transmission medium terminated to physically secure location at both ends.

Excerpt from Section **5.10.1.2.1 Encryption for CJI in Transit**

Encryption shall not be required if the transmission medium meets all of the following requirements:

- The agency owns, operates, manages, or protects the medium.
- Medium terminates within physically secure locations at both ends with no interconnections between.
- Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
- Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
- With prior approval of the CSO.

TO FIPS OR NOT TO FIPS

When working with compliance requirements of all kinds, from HIPAA to ITAR to CJIS, our Compliance Team recommends limiting the scope of privileged data to reduce the burden of maintaining compliance. From a planning perspective, this means less complex and less expensive infrastructure.

In the Village's case, putting policies in place that prevent CJI from leaving the boundary of the internal network means that your firewall does not need FIPS 140-2 encryption for its VPN connections. We recommend placing the following restrictions in place to limit the scope of FIPS requirements:

1. Restrict file transfer and disable clipboard for remote connections from PD laptops to PD workstations so that CJI cannot be transmitted across the client VPN connection. This policy can be implemented and enforced at any time through Active Directory.
2. Prevent devices on the DPW network from being able to communicate with anything on the Livingston County switch. This restriction requires Phase Two to be completed so that the Village and PD networks are fully separated. Right now, they are all on the same network, so this type of network-based restriction isn't possible.

Please keep in mind that the CJIS Security Policy is updated one to two times per year. Standards, requirements, and controls could change. The most resent revision, 5.9.4 is already talking about FIPS 140-3 and states that FIPS 140-2 certificates will not be acceptable after September 21, 2026.

Brightline recommends doing both – adopting policies and access controls to limit the scope of compliance AND future-proofing the Village's infrastructure against future changes to CJIS Security Policy by investing in a firewall with FIPS-validated cryptography.

Cisco Meraki (FIPS Certificate #4036)

Cisco takes a very holistic approach to FIPS compliance by creating a universal cryptographic module and implementing it across all their security platforms. That way, they only need to put one module through the validation process and one certificate applies to all of their security products.

Phase Two includes a Meraki switch and Phase Four includes Meraki access points. Adding Meraki firewalls allows the Village's network to be managed with a single pane of glass. Furthermore, Cisco Meraki for Government is now available to enable FIPS-compliant management.

COST ESTIMATES

Recurring Costs

- 3-year Licensing & Support - $5,500
  **1 or 5-year licensing available upon request*

One-Time Costs

- Firewall Hardware (Village Hall & DPW) - $2,000
- Deployment - $6,750

PHASE FOUR: WiFi Upgrade

CURRENT ACCESS POINTS

Your current WiFi is provided by Ubiquiti UniFi access points. Ubiquiti products are considered to me “prosumer” products in that they are consumer-grade products with enterprise features. They’re fantastic products for the home networks of people who know what they’re doing, but we do not recommend them to customers. Especially not for customers with any regulatory compliance requirements. Also, Ubiquiti is Chinese company with all hardware made in China.

CISCO MERAKI

We recommend Cisco Meraki for its ease of management, price point and regulatory compliance. Cisco is a US-based company, and all parts and products are TAA Compliant. Furthermore, Cisco Meraki for Government is now available to enable FIPS-compliant management. FIPS-compliant encryption for access and authentication to the management interface of wireless access points is required by the CJIS Security Policy. While this requirement can be mitigated with wireless network access controls, it’s worth having it to help future-proof the Village’s network.

Excerpt from Section **5.13.1.1 802.11 Wireless Protocols**

Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g., SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.

COST ESTIMATES

NOTE: The DPW firewall from Phase Three will have built-in WiFi.

Recurring Costs

- 3-year Licensing & Support - $1,000
  **1 or 5-year licensing available upon request*

One-Time Costs

- Two (2) Access Points - $1,000
- Deployment - $2,000

PROJECT TOTALS

PHASE		Upfront Cost	Recurring Cost
1	**EVENT LOGGING** Temporary Server Lease ($250/month) NeQter Compliance Engine Deployment & Training	$ 5,070	$ 4,320 yearly or $10,800 3-years
2	**NEW SERVER / NETWORK SEGMENTATION** New Server New Switch Rack & Power Secondary Domain Controller Licensing Deployment & Migration	$ 38,400	$ 100 monthly + $350 3-years
3	**FIREWALL UPGRADE** Firewall Hardware Advanced Security Licensing, FedRAMP Deployment	$ 8,750	$5,500 3-years
4	**WIFI UPGRADE** Two (2) Access Points Enterprise Licensing, FedRAMP Deployment	$ 3,000	$1,000 3-years

UPFRONT TOTAL – ALL PROJECTS	**$ 55,220**
RECURRING TOTAL – ALL PROJECTS (3-YEAR TERMS)	**$ 17,650**

brightlineIT

THANK YOU!

FOR PARTNERING WITH US

10355 Citation Dr.
Brighton, Michigan 48843
info@brightlineit.com
www.brightlineit.com