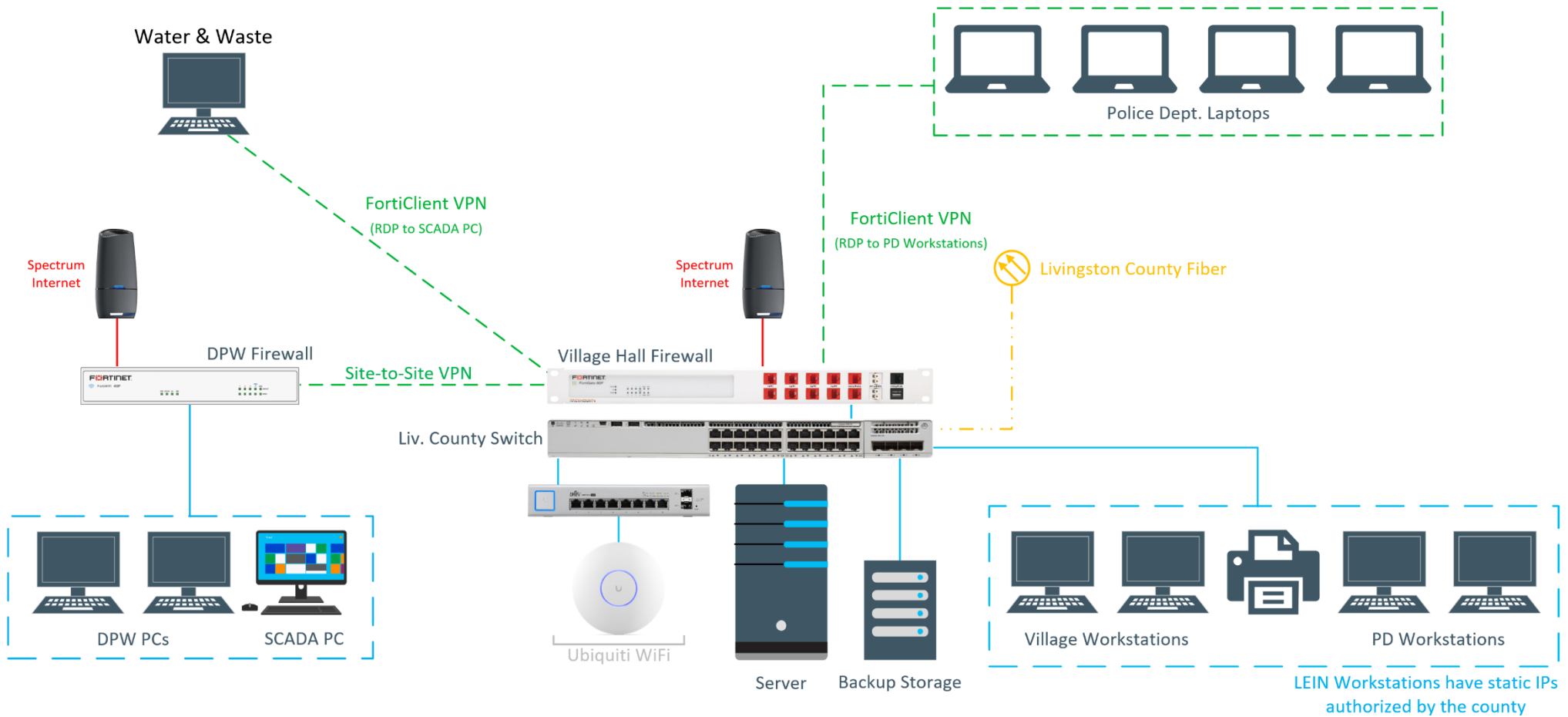
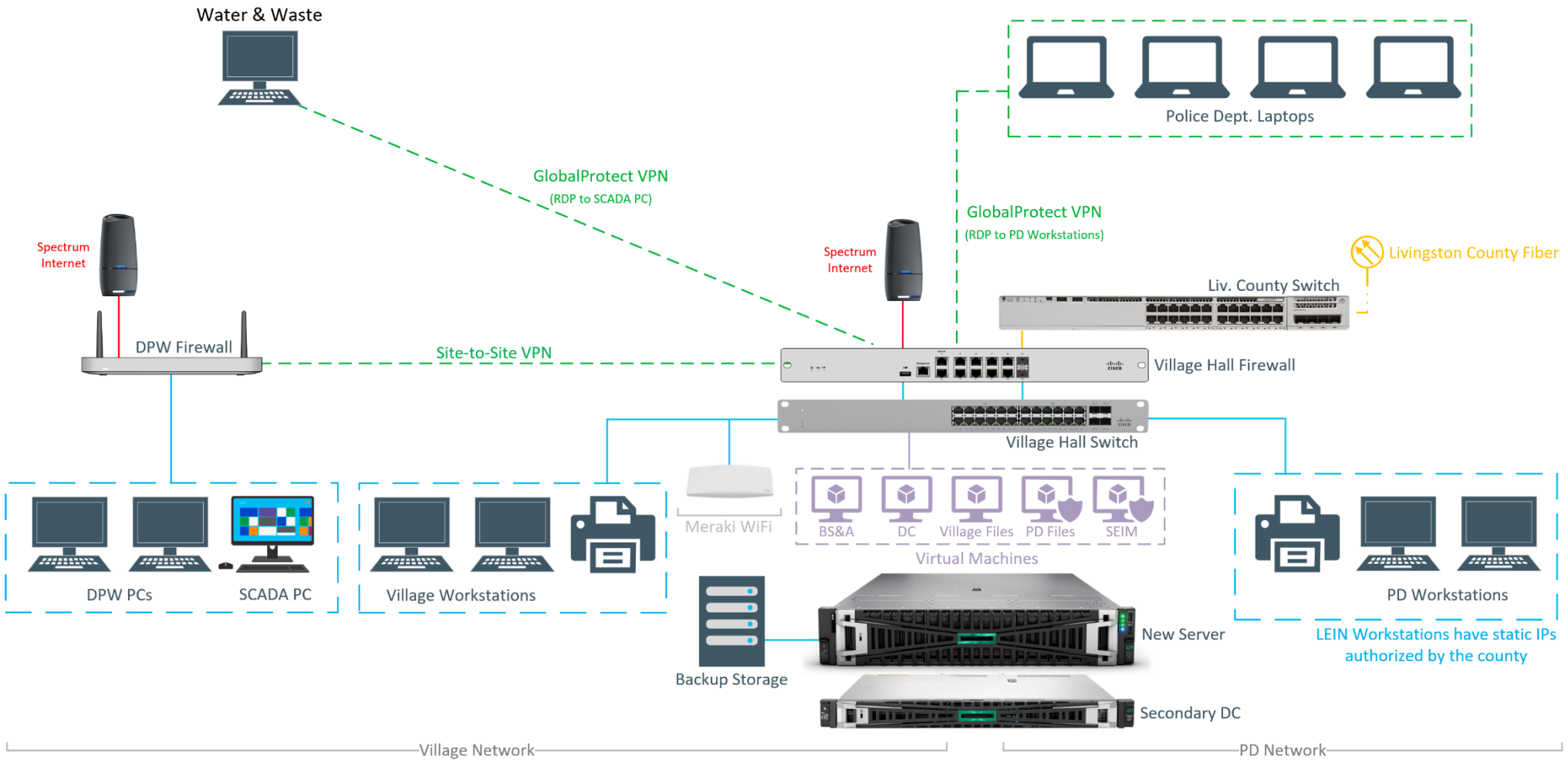


APPENDIX A – Current Infrastructure



APPENDIX B – Proposed Infrastructure



APPENDIX C – Cisco Meraki, FIPS Certificate #4036

Module Name	Cisco FIPS Object Module																										
Standard	FIPS 140-2																										
Status	Active																										
Sunset Date	1/5/2026																										
Overall Level	1																										
Caveat	When installed, initialized and configured as specified in the Security Policy Section 3 and operated in FIPS mode. No assurance of the minimum strength of generated keys																										
Security Level Exceptions	<ul style="list-style-type: none"> • Design Assurance: Level 3 • Mitigation of Other Attacks: N/A 																										
Module Type	Firmware																										
Embodiment	Multi-Chip Stand Alone																										
Description	The Cisco FIPS Object Module (FOM) is a firmware library that provides cryptographic services to a vast array of Cisco's networking and collaboration products. The module provides FIPS 140 validated cryptographic algorithms for services such as IPSEC, SRTP, SSH, TLS, 802.1x, etc. The module does not directly implement any of these protocols, instead it provides the cryptographic primitives and functions to allow a developer to implement the various protocols.																										
Approved Algorithms	<table border="0"> <tr> <td>AES</td> <td>Cert. #A1420</td> </tr> <tr> <td>CKG</td> <td>vendor affirmed</td> </tr> <tr> <td>CVL</td> <td>Cert. #A1420</td> </tr> <tr> <td>DRBG</td> <td>Cert. #A1420</td> </tr> <tr> <td>DSA</td> <td>Cert. #A1420</td> </tr> <tr> <td>ECDSA</td> <td>Cert. #A1420</td> </tr> <tr> <td>HMAC</td> <td>Cert. #A1420</td> </tr> <tr> <td>KAS-SSC</td> <td>Cert. #A1420</td> </tr> <tr> <td>KBKDF</td> <td>Cert. #A1420</td> </tr> <tr> <td>RSA</td> <td>Cert. #A1420</td> </tr> <tr> <td>SHA-3</td> <td>Cert. #A1420</td> </tr> <tr> <td>SHS</td> <td>Cert. #A1420</td> </tr> <tr> <td>Triple-DES</td> <td>Cert. #A1420</td> </tr> </table>	AES	Cert. # A1420	CKG	vendor affirmed	CVL	Cert. # A1420	DRBG	Cert. # A1420	DSA	Cert. # A1420	ECDSA	Cert. # A1420	HMAC	Cert. # A1420	KAS-SSC	Cert. # A1420	KBKDF	Cert. # A1420	RSA	Cert. # A1420	SHA-3	Cert. # A1420	SHS	Cert. # A1420	Triple-DES	Cert. # A1420
AES	Cert. # A1420																										
CKG	vendor affirmed																										
CVL	Cert. # A1420																										
DRBG	Cert. # A1420																										
DSA	Cert. # A1420																										
ECDSA	Cert. # A1420																										
HMAC	Cert. # A1420																										
KAS-SSC	Cert. # A1420																										
KBKDF	Cert. # A1420																										
RSA	Cert. # A1420																										
SHA-3	Cert. # A1420																										
SHS	Cert. # A1420																										
Triple-DES	Cert. # A1420																										

APPENDIX D – Cisco Meraki for Government, FedRAMP Authorization



Package ID

FR2315535023

Package Request Form

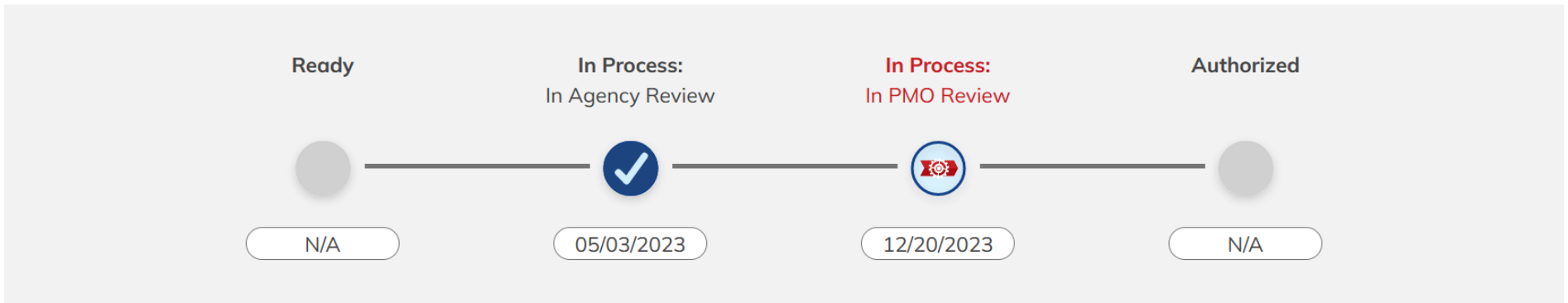
Authorizations ⓘ

1

Reuse ⓘ

1

Authorization Status ⓘ



Authorization Details ⓘ

Authorization Type: Agency
FedRAMP Ready: No FRR Date
JAB Review: Not Active
Agency Review: 05/03/2023
PMO Review: 12/20/2023
FedRAMP Authorized: Not Active
Annual Assessment: N/A
Independent Assessor: Coalfire Systems, Inc.

System Profile ⓘ

Service Model: SaaS
Deployment Model: Government Community Cloud
Impact Level: Moderate

Dependent Products ⓘ

N/A