SPRINGFIELD
SCHOOL DISTRICT

Superintendent of Schools
Peter Burrows, D.Ed.
(802) 885-5109

Director of Curriculum
Alena Martes
(802) 885-5112

Director of Student Services
Courtney Dextraze-Wiese
(802) 885-5117

Chief Financial Officer
Rick Pembroke
(802) 885-8391

301 South Street · Springfield, Vermont · 05156 · http://www.ssdvt.org

Amendment to:
FY 2027 Final Form 470

SPRINGFIELD SCHOOL DISTRICT
ATTENTION: MARK SCHMITT, IT DIRECTOR
301 SOUTH STREET
SPRINGFIELD, VT 05156

Contents

CATEGORY TWO SERVICE REQUESTS – ADDITIONAL DETAILS 2
1. Service Type: Internal Connections 2
1.1. Function: Cabling 2
2. Service Type: Internal Connections / Basic Maintenance of Internal Connectors 2
2.1. Function: Wireless access point and necessary software and licenses / Wireless Controllers and Necessary Software and Licenses 2
3. Service Type: Internal Connections / Basic Maintenance of Internal Connectors 2
3.1. Function: Uninterruptable Power Supply/ Battery Backup and Necessary Software and Licenses 2
Attachment 1: Network infrastructure equipment and management (ref.: 2.2.4) 3
1. Priorities and success criteria 3
2. Use cases: centralized management and configuration (Priority 1) 3
3. Use cases: network health and outage monitoring (Priority 2) 4
4. Use cases: network security management (Priority 3) 5
5. Use cases: AI-assisted network repair (Priority 4) 6

CATEGORY TWO SERVICE REQUESTS – ADDITIONAL DETAILS

1. Service Type: Internal Connections
   1.1. Function: Cabling
   1.2. Manufacturer: No Preference
   1.3. Entities: 4
   1.4. Quantity: 1000
   1.5. Unit: Feet
   1.6. Additional Details: We are seeking four (4) boxes or spindles of Cat6e shielded ethernet cable. Each unit should be 1000 feet in length. Preference is for blue to maintain standard.

2. Service Type: Internal Connections / Basic Maintenance of Internal Connectors
   2.1. Function: Wireless access point and necessary software and licenses / Wireless Controllers and Necessary Software and Licenses
      2.1.1. Addendum: Network infrastructure management and support
   2.2. Manufacturer: Current Wireless equipment and management provided by Extreme networks
      2.2.1. Addendum: Current Wireless equipment details:
         2.2.1.1. 9x Extreme Networks 5420F Switch
         2.2.1.2. 118x Extreme Networks Wireless Access Points: AP460C, AP410C, or AP510C
      2.2.2. Addendum: Current network infrastructure
         2.2.2.1. ~50x HPE Aruba 2540 or 2930 switches
      2.2.3. Addendum: Wireless network management
         2.2.3.1. Extreme Networks ExtremeCloud IQ
      2.2.4. Additional Details: See attached use case document.

3. Service Type: Internal Connections / Basic Maintenance of Internal Connectors
   3.1. Function: Uninterruptable Power Supply/ Battery Backup and Necessary Software and Licenses
   3.2. Manufacturer: Current UPS: ~12x APC 2200XL (batteries recently refreshed)
      3.2.1. Additional details:
         3.2.1.1. Must have requirements: 20-minute run time; rack mountable
         3.2.1.2. Preferred requirements: Network manageable; power outage notification (SMS and/or email); power load reporting (via dashboard); line conditioning

Attachment 1: Network infrastructure equipment and management (ref.: 2.2.4)

1. Priorities and success criteria

Priority	Goal	Proposed success measure
1. Centralized management and configuration	Every switch and AP inventoried and managed (or at least visible) from one console	100% of devices discovered and inventoried; configuration backups for 100% of district-owned switches; standard change pushed to all switches in under 1 hour
2. Network health and outage monitoring	Know about outages before users call	Device-down alerts within 5 minutes; 90% of outages detected by monitoring before a help desk ticket; monthly uptime report per building
3. Network security management	Reduce attack surface and prove controls are in place	All switches on supported firmware within 90 days of release of critical fixes; no default credentials; unauthorized devices flagged within 15 minutes; audit-ready change log
4. AI-assisted network repair	Contain common outages automatically until IT staff fixes the root cause	Common outages (hung ports, loops, failed uplinks with backup paths) contained within 10 minutes; 100% of automated actions logged and ticketed

2. Use cases: centralized management and configuration (Priority 1)

ID	Use case	Trigger	Expected outcome	Need
CM-01	Discover and inventory all network devices	Initial deployment; scheduled weekly re-scan	Complete list of every switch and AP with vendor, model, serial, firmware, IP, MAC, building, closet, and owner (district or vendor)	Must
CM-02	Single console for multi-vendor view	Daily operations	Critical network devices shown together by building, with clear ownership labels	Must
CM-03	Back up configurations automatically	Nightly schedule; any detected change	Versioned config history for every owned switch, restorable in minutes	Must
CM-04	Apply standard templates	New switch install; policy change	VLANs, SNMP, NTP, syslog, AAA, and banner settings pushed consistently to groups of switches	Must
CM-05	Detect configuration drift	Config differs from template or golden copy	Alert listing the device and exact lines that changed	Should
CM-06	Zero-touch provisioning of replacements	Failed switch replaced	New switch plugged in pulls its configuration with no console cable	Should

ID	Use case	Trigger	Expected outcome	Need
CM-07	Bulk port and VLAN changes	Classroom move, new lab, summer reconfiguration	Change many ports across buildings in one task, with preview before commit	Should
CM-08	Firmware lifecycle management	New release or advisory	View firmware by device, stage upgrades, schedule them off-hours, roll back on failure	Must
CM-09	Role-based access	Onboarding staff or vendor	Admins, building techs, help desk, and vendor see only what their role allows	Must
CM-10	Asset lifecycle and lease tracking	Budget planning; lease renewal	Report of end-of-support dates, warranty, and lease terms per device	Should

Example flow, CM-01 Discover and inventory:

1. Administrator enters seed IPs or subnets and provides read-only SNMP and SSH credentials.
2. Solution scans and uses LLDP/CDP neighbor data to find connected switches and APs.
3. Solution classifies each device by vendor and model and asks the administrator to confirm owner (district or vendor) and location.
4. Devices the solution cannot reach or identify are listed as exceptions for follow-up.
5. Administrator exports the inventory as the district's baseline count and schedules weekly re-discovery.

3. Use cases: network health and outage monitoring (Priority 2)

Monitoring must cover leased gear as well as owned gear.

ID	Use case	Trigger	Expected outcome	Need
HM-01	Real-time device up/down monitoring	Device stops responding	Alert by email, SMS, or app within 5 minutes, naming device, building, and closet	Must
HM-02	Building-level health dashboard	Daily check; incident	One screen showing each of the 4 buildings as green, yellow, or red	Must
HM-03	Root-cause and dependency awareness	Upstream link fails	One alert for the failed uplink instead of dozens for every switch behind it	Must
HM-04	Interface and uplink utilization	Threshold exceeded; capacity planning	Graphs and alerts for saturated uplinks, errors, and discards	Must
HM-05	PoE budget monitoring	PoE nearing capacity	Warning before APs, phones, or cameras lose power	Should
HM-06	Wireless health and	Complaints of slow Wi-Fi; testing windows	AP status, client counts, channel utilization, and interference per building	Must

ID	Use case	Trigger	Expected outcome	Need
	client experience			
HM-07	Environmental and hardware alerts	Fan, power supply, or temperature fault	Alert before a closet overheats or a PSU failure	Should
HM-08	Historical uptime and SLA reporting	Monthly	Uptime per building and per vendor	Must
HM-09	Planned maintenance windows	Scheduled change	Alerts suppressed during the window	Should
HM-10	Critical-period readiness	State testing, MAP, or other online assessments	Heightened alerting and pre-test health check for testing locations	Should
HM-11	Escalation and ticket integration	Alert raised	Ticket created automatically in the district help desk system	Should

Example flow, HM-03 Root-cause awareness:

1. The fiber uplink between Building B and the district core fails.
2. Solution detects the core-side interface down and loses contact with all Building B switches and APs.
3. Using the topology map, it raises one critical alert: "Building B uplink down; 14 dependent devices unreachable."
4. Help desk sees Building B as red on the dashboard and answers incoming calls with a known cause.
5. When the link recovers, the solution confirms all dependent devices are back and logs outage duration for the monthly report.

4. Use cases: network security management (Priority 3)

ID	Use case	Trigger	Expected outcome	Need
SM-01	Centralized administrator authentication	Admin logs in to any switch or the console	Login through RADIUS/TACACS+ or directory (Azure AD/Entra ID or Google) with MFA; no shared local passwords	Must
SM-02	Audit trail of every change	Any configuration change	Who changed what, when, and from where, retained for at least 90 days	Must
SM-03	Rogue and unknown device detection	Unknown device connects to a port or rogue AP appears	Alert with port, building, and MAC; option to shut the port	Must
SM-04	Network access control	Device joins wired or wireless network	Students, staff, guests, IoT (cameras, HVAC, displays), and infrastructure placed in separate VLANs or roles automatically	Should

ID	Use case	Trigger	Expected outcome	Need
	and segmentation			
SM-05	Vulnerability and firmware advisories	Vendor publishes a security advisory	Affected devices listed automatically with recommended fix	Should
SM-06	Configuration compliance checks	Scheduled audit	Report flagging Telnet enabled, default SNMP communities, unused ports active, weak passwords, missing banners	Must
SM-07	Port security for classrooms and public areas	Device swapped on a classroom port	Port limits, BPDU guard, DHCP snooping, and unused-port shutdown enforced by template	Should
SM-08	Log forwarding to SIEM or security partner	Security event on any device	Syslog and alerts sent to the district SIEM, SOC, or MS-ISAC/CIS service	Should
SM-09	Vendor access control	Leasing vendor needs to make a change	Each outside party accesses only its own devices; with MFA, logging, and time-limited access	Must
SM-10	Incident isolation	Infected or compromised device detected	Quarantine the device or port in one action from the console	Should

Example flow, SM-03 Rogue device detection:

1. A personal wireless router is plugged into a classroom wall jack in Building A.
2. Solution detects a new MAC address that is not in inventory, and the wireless system detects an unauthorized SSID broadcasting nearby.
3. Solution alerts the network administrator with the switch, port number, and building.
4. Administrator shuts the port from the console.
5. The event is logged for the security report.

5. Use cases: AI-assisted network repair (Priority 4)

AI-assisted repair restores service within minutes using small, reversible actions, then hands the root cause to IT staff with a diagnosis.

ID	Use case	Primary actor	Trigger	Expected outcome	Need
AR-01	Automated diagnosis	Solution (AI engine)	Outage or degradation alert	Alerts, topology, logs, and recent changes correlated into a probable cause with a confidence level and plain-language summary	Must
AR-02	Restart a failed port or PoE device	Solution (AI engine)	AP, phone, or camera stops responding on a known port	Port or PoE power cycled automatically; device confirmed back online	Must

ID	Use case	Primary actor	Trigger	Expected outcome	Need
AR-03	Fail over to a redundant path	Solution (AI engine)	Uplink or link failure where a backup path exists	Traffic moved to the backup link; degraded state shown on the dashboard	Should
AR-04	Roll back a change linked to an outage	Network administrator (approves)	Outage starts shortly after a configuration change	Last known-good configuration restored from CM-03 backups	Must
AR-05	Contain a loop or broadcast storm	Solution (AI engine)	Spanning-tree loop or storm detected	Offending port shut or rate-limited before the building network collapses	Must
AR-06	Cover a wireless gap	Solution (AI engine)	AP fails in a classroom area	Neighboring APs adjust power and channel to cover the gap	Should
AR-07	Hand off root cause to IT	Network administrator	Any automated action taken	Ticket opened with timeline, actions taken, current state, and recommended permanent fix	Must
AR-08	Learn from resolved incidents	Network administrator	Incident closed	Suggested new or improved runbooks based on what fixed similar past incidents	Should

Guardrails decide which actions run on their own:

Tier	Example actions	Approval
Automatic	Port or PoE restart, loop containment, failover to an existing backup path	None; staff notified immediately
Approve first	Configuration rollback, wireless re-tuning, any action affecting a whole building	One-tap approval by an administrator on mobile; falls back to recommend-only if no answer in 10 minutes
Recommend only	Firmware changes, security quarantine (SM-10) without a written agreement	Staff or the owning vendor carries out the action

Additional rules: limit repeat actions (for example, no more than 2 attempts per device per hour, then escalate); pause automation during maintenance windows and testing periods unless enabled; give administrators a district-wide off switch; and keep every action in the SM-02 audit trail.

Example flow, AR-02 and AR-07:

1. At 7:40 a.m., an AP in a Building C classroom stops responding.
2. The solution sees the switch port is up but the AP is not drawing normal PoE power, and diagnoses a hung AP with high confidence.
3. It power-cycles the port; the AP returns in 3 minutes and clients reconnect.
4. The solution opens a ticket noting this AP has hung 3 times in 30 days and recommends replacement or a firmware check.
5. The network administrator reviews the ticket and schedules the permanent fix.