## Supply Chain Risk Management per NIST Core V1.1 / NIST 800-171 / NIST 800-53 R5

**Process**

* Have an acquisition process that shows business process, data flows and Single Point of Failure
* How do you apply vendor unique features into Frontier Local School District (FLSD) requirements?

**Vendor selection committee meets to review vendors**

* Vendor’s compliance to FLSD policies
* Vendor’s certifications to industry cybersecurity requirements
* Vendor’s cybersecurity Risk Assessment
* Vendor’s signed NDA
* Vendors Business Continuity Plan
* Vendor’s current (within the last year) penetration test - passed
* Identify the subcontractors used by the vendor
* Plan if the vendor loses and cannot restore data
* Third party plan for Incident Response event written and in the Service Agreement

**FLSD Implementation**

* FLSD Risk assessment control for using the third-party vendor
* FLSD Vulnerability assessment of the third-party vendor system / software
* Review and update the FLSD Supply Chain Risk Management Plan to address threat, organizational or environmental changes
* Define roles and responsibilities for the new Vendor in the Incident Response plan
* Utilize vendor diversity to eliminate Single Point of Failure issues
* Monitor and report the effectiveness of the vendor
* Identify and document the processes and skillset required to replace the vendor if they cannot perform
* Have a plan to verify genuine systems and not altered systems modified to listen to our system
* Have operational testing of the vendor system /software in use
* Inspect a sample of the Vendor system / software at random intervals
* Have configurations of system reviewed, updated before IR rehearsal and execution
* What is the method used to verify that the vendor meets the requirements
* Show documented evidence of vendor monitoring
* Report of any vendor failures in the last 12 months
* Last inspection of the vendor audit report
* List of non-conformances and Corrective Actions report
* Management review of the vendor in the last 12 months
* Show the last 12 months of communication to the vendor
* Show the quality reports communicated to the vendor