



Content Filtering & Student Safety RFP Pre-Bid Meeting

August 17, 2020
Virtual Meeting



Delaware
Department of Education



Meeting Logistics

- Please type the following into the Chat:
 - Name
 - Title
 - Organization
 - Phone number
 - Email
- Keep microphones muted. We will open the meeting for questions at the conclusion of the presentation



Introductions

Delaware Department of Education (DDOE):

Dr. Alyssa Moore: Education Associate, Digital Learning

Patches Hill: Director, Technology Operations

Meaghan Brennan: Education Associate, Financial Reporting and Contracting

Delaware Department of Technology and Information (DTI):

Caleb Bontrager: Lead Telecom Technologist

Red Clay Consolidated School District:

Tony Clemmons: Network Coordinator



Agenda

- Overview
- Requirements & Scope of Work
- Accessibility
- Proposal Dates & Application Package
- Questions



Overview



Delaware
Department of Education



Overview

- Intent of this Request for Proposal is to:
 - Provide a scalable, cost-effective, subscription based content filtering and student safety solution
 - Provide a content filtering solution for devices, used by students and staff, when they are both on and off the state network
 - Provide monitoring and alert services for student behavior self-harm and threat detection
 - Provide Internet security, threat detection, and response capability/blocking
 - Provide multiple layers of reporting capability for varied audiences (ex. technicians, school staff, and families)
 - Provide multi-layered access to system features
 - Provide the capability to manage the solution from the Cloud



Shared Controls

- The solution will be utilized by the state as a whole in partnership with the Department of Technology and Information, the Department of Education, and Delaware districts and charter schools.
- The Content Filtering Solution must be able to provide services both on and off the state network.
- The Content Filtering Solution must support all users and roles, including DDOE staff, DTI staff, district/charter technology administrators, district/charter leadership, teachers, students, and parents/guardians. The system must be flexible enough to accommodate future population groups and roles as they are identified.



Technical Environment

- Technical environment is engineered and managed in a shared model cooperatively between DTI, DDOE, and the individual districts and charter schools
- Filtering controls are implemented with URL filtering using proxy appliances deployed centrally in an explicit and in-line model
- K-12 network serves around 300 sites. Each site is connected to the two State data center locations via private TLS circuits in a hub/spoke model
- DTI runs the core network and WAN/L2 Switching infrastructure, wireless infrastructure is implemented and managed by the individual districts/charters independently from DTI
- DTI runs a central Active Directory Forest. Some districts use other 3rd party platforms for authentication
- Each district/charter is responsible for managing their endpoints on the network
- “On network” is considered to be any end point that is connected to the K-12 education network. All other locations are considered to be “off network”
- Districts/charters need the ability to differentiate policy and services as per the needs of their environments



Requirements & Scope of Work



Delaware
Department of Education



Filtering

- Categorization should accommodate PreK-12 learning needs
- Categorization should be hierarchical in nature and have sub-categorization
- Policies should be able to be configured independently for on network and off network environments and filtering should be able to be scheduled
- DDOE & DTI needs to be able to enforce minimum baseline CIPA policy
- Policy should support delegation of access to districts/charters to manage their policy sub section
- Support different policies for different user types/groups
- Support detailed technical logging, logging for troubleshooting, and for auditing compliance



Monitoring & Reporting

- Reporting data must be:
 - Available “live” as traffic occurs; details are recorded and available for review
 - Exportable
 - Selectable based on filters (source IP, user initiating traffic, on/off network, time of day, time range, etc.)
 - Able to provide top sites visited, separated by user, building, and district levels
- Data must be retained for 13 months
- Support export of network/technology security events to Splunk
- Provide for an "end user behavior" or a non-technical view of log data (user browsed these sites), as well as a forensic detail view of all http(s) communication (all connections, not just the main site that was accessed)



Monitoring & Reporting

- Student safety/self-harm protection (inclusive of but not limited to):
 - Communication processes for school district staff when student safety triggers occur
 - Communication with law enforcement
 - Communication with parents
 - Variation of response based on trigger/risk level
 - Systems that are actively monitored
 - Live review of alerts and who is responsible for the review
 - Ability to flag student and school safety concerns
 - Process for avoiding false positive self-harm triggers
 - Ability to compartmentalize by district/charter
 - Ability to configure at district/charter level



Compatibility & BYOD

- Support various operating systems with full functionality:
 - iOS
 - Android OS
 - Chrome OS
 - Mac OS
 - Windows OS
- Provide an approach to filtering/monitoring/reporting BYOD devices for various users
- Support filtering enforcement on unmanaged and unauthenticated endpoint devices while they are connected to on-prem networks without requiring client proxy configuration
- Support safe search enforcement of search engines and YouTube for unmanaged devices while on network and for unmanaged devices without SSL interception



Management

- Support configuration management of all areas of the platform via API, preferably with vendor created and supported Ansible Modules
- Ability to handle multi-tenancy with central and delegated administration based on organizational groupings
- Ability to be managed through a cloud-based, browser agnostic dashboard



Security

- Ability to prevent users from circumventing filtering controls
- Ability to delegate controls to different segments of the multi-tenant environment
- Support various authentication types (ex. SAML (including ADFS), OAuth, Google, and ClassLink)
- Ability to detect and block proxy anonymizer services
- Support categorization methodology
- Ability to apply custom categories and/or override a category applied to a given website
- Provide for custom blocked and allowed lists that are applied at the state, district, and school levels
- Support classification of uncategorized websites
- Utilize readily available domain and IP blacklists sourced from common sources in content filtering and categorization (ex. US Cert, MS-ISAC, SpamHaus, and other open source feeds)



Security

- Provide malware protection
- Support the termination and inspection of SSL traffic
- Provide the flexibility to disable or enable SSL decryption for web traffic destined for sensitive categories
- Provide the following certificate inspection capabilities: expiration dates, revocation status (CRL & OCSP), common name mismatches, self-signed certificates, alternate name matches, wildcard certificate verification
- Support SSL Interception whitelist management
- Detect command and control callbacks
- Enforce protocol validation to ensure communication is standard HTTP or TLS on respective ports
- Provide application control of web applications
- Ability to control access to parts of an approved site (ex. Access to channels in YouTube)
- Ability to provide granular access control within approved categories



Capacity & Bandwidth Management

- Provide fault tolerance and resilience across geographic locations throughout the country
- Ability to scale over time as the load increases
- Ability to do Quality of Service when on network and prioritize educational content
- Ability to prioritize specific users based on directory system group membership and location
- Ability to manage quotas and/or prioritize traffic based on web applications or website domains



End Users

- Staff

- Districts/charters should be able to customize the ability for teachers/staff to override specific websites in allowed configured/blocked categories during a specific session or time-frame
- Provide logging of any temporary override
- Provide alerts
- Ability to integrate with Student Information System or Learning Management System
- Ability for teachers to simulate student policy
- Ability to apply differentiated policies by user groups

- Students

- Ability to identify the policy and category that blocks actions as well as ability to identify vendor when traffic is blocked including details to address misidentification
- Ability to apply custom messaging to blocked pages
- Support re-categorization requests



End Users

- Parents/Guardians
 - Ability to make policies more restrictive and get reports on student activity
 - Portal should allow for ability to control off-site filtering
 - Support features should not impact district/charter helpdesk
 - Support self-service for password resets
 - Support account creation via Student Information System
 - Provide automated process for linking parent/guardian accounts with appropriate student accounts
 - Allow for restrictions in addition to district/charter settings based on location of the device, school days, and time-frames
 - Ability for districts/charters to configure parent/guardian reporting criteria
 - Ability for district/charters to override parent restrictions as needed
 - Ability for districts/charters to customize information included in parent summary of daily student activity
 - Ability for districts/charters to customize parent notification of student safety event flags
 - Ability to log acknowledgement of any alerts sent to and received by parents/guardians



Support

- Provide support model including assignment of point personnel who have knowledge of our environment and can provide individualized support
- Provide the ability to support end users
- Provide a toolset to analyze and troubleshoot connectivity and presentation issues
- Capability to diagnose, test, and resolve issues with specific websites or web applications with minimal involvement from the state of DE
- Provide causal analysis for issue resolution



Accessibility



Delaware
Department of Education



Accessibility

- The solution must meet the standards of Section 508 of the Rehabilitation Act of 1973, which includes the Web Content Accessibility Guidelines 2.0 (WCAG 2.0). Information about Section 508 is available from the GSA (<https://www.section508.gov>). Information about WCAG 2.0 is available at the W3C website. (<https://www.w3.org/TR/WCAG/>).



Proposal Dates and Application Package



Delaware
Department of Education



Important Dates

Public Notice	August 6, 2020
Deadline for Questions	August 21, 2020
Response to Questions Posted By	August 28, 2020
Deadline for Receipt of Proposals	September 9, 2020 at 2:00 PM (Local Time)
Estimated Notification of Award	October/November 2020



Complete Application Package

Four paper copies with one marked “original” with original signatures and two electronic copies on a USB stick

- Transmittal Letter as specified on page 1 of the Request for Proposal including an Applicant's experience, if any, providing similar services.
- The remaining vendor proposal package shall identify how the vendor proposes meeting the contract requirements and shall include pricing. Vendors are encouraged to review the Evaluation criteria identified to see how the proposals will be scored and verify that the response has sufficient documentation to support each criteria listed.
- One (1) complete, signed and notarized copy of the non-collusion agreement (See Attachment 2). “ORIGINAL”, MUST HAVE ORIGINAL SIGNATURES AND NOTARY MARK. All other copies may have reproduced or copied signatures – Form must be included.
- One (1) completed RFP Exception form (See Attachment 3) – please check box if no information – Form must be included.
- One (1) completed Confidentiality Form (See Attachment 4) – please check if no information is deemed confidential - Form must be included.
- One (1) completed Business Reference form (See Attachment 5) – please provide references other than State of Delaware contacts – Form must be included.
- One (1) complete and signed copy of the Subcontractor Information Form (See Attachment 6) for each subcontractor - only provide if applicable.
- One (1) completed Vendor Response document in MS Excel format (See Appendix C).



RFP Designated Contact

Meaghan Brennan

Education Associate, Financial Reporting and Contracting

DE Department of Education, Finance Office, Rm. 275
401 Federal St, Ste 2
Dover, DE 19901

Meaghan.Brennan@doe.k12.de.us



Communications made to other State of Delaware personnel or attempting to ask questions by phone or in person will not be allowed or recognized as valid and may disqualify the vendor. Vendors should rely only on written statements issued by the RFP designated contact (above).



Questions



Delaware
Department of Education



Questions

- Methods for asking questions:
 - Use the Raise Hand feature to ask your question aloud during this portion of the meeting
- OR**
- Type your question in the Chat

