CITY OF SANTA BARBARA

LIBRARY BOARD REPORT

AGENDA DATE: March 11, 2021

TO: Library Board

FROM: Administration Division, Library Department

SUBJECT: Cisco Umbrella (attachment 2)

DISCUSSION:

SBPL proposes to to use the Cisco Umbrella web-based product to ensure it adheres to CIPA compliance. Umbrella is a cloud-delivered enterprise network security system that monitors and prevents cyber security threats as well as provides a secure internet gateway against internet sites that are either obscene, pornographic, or harmful to minors. In that sense, it also functions as a web content filter. Umbrella is managed via a cloud-based dashboard that would be administered by library technology staff. Cisco Umbrella comes with a stock blacklist (denied) and whitelist (allowed) based on Cisco's database of websites. Known pornographic sites, for example, are put in the blacklist, i.e their Internet Protocol (IP) ranges are put in that list.

Umbrella will filter Black Gold IP ranges for both its wired and Wi-Fi internet networks at all branches. This will include both the hardwired computers as well as patrons' own devices that they bring into the library. Umbrella will not actively track who patrons are and what they are doing; it will simply allow access to sites that are whitelisted and deny access to those that are blacklisted. These lists are updated weekly, if not daily, by Cisco. SBPL technology staff will have the ability to add sites to the blacklists (e.g. if a new obscene site is discovered) as well as move sites to the whitelists (e.g. a site about health research that mentions human anatomical parts in the blacklist) as necessary.

Should a patron want to anonymously request access to a blocked site by means of a specific device, that access can be granted via Umbrella. Umbrella will have a customized "blocked page" that will alert a patron that they tried to access a blocked site. Should an adult patron want to request access to it, they would click on a link to a separate form that will have a submission field for the requested site (required), purpose for the site to be viewed (required), user's email (required), name (optional), and IP address (automatically filled in if it's on a wired computer or via the user's own device over Wi-Fi). SBPL technology staff would receive the request via email and evaluate it in conjunction with the library's Internet Use and Safety Policy and with library administration if necessary. Should the site still be required to be blocked for all patrons but access be granted for this specific patron, the patron would receive a blocked site bypass code, designed to time out at the end of the day, as an email response. Should

the site still not be deemed appropriate even to the specific patron, the patron will receive an email that states access was denied.

Should a patron want to request access to a blocked site and want to identify themselves, they may send an email message to a City of Santa Barbara email account that is monitored by technology staff. Or they submit their request in-person to library staff. They may also request a blocked site be accessed anonymously via email. All requests will be routed to the library's technology staff, who will run them through the evaluation procedures noted above.

Cisco Umbrella will not track patron usage and logs will not be compiled with user information embedded in them. In no way will Umbrella be used to intrude on patron privacy. It will only provide compiled statistics, from all devices on the network, for overall categories accessed. Examples would be the number of times social media, streaming sites, email sites, or web browsing occurred.

Having direct control over the library's web filtering content software would eliminate a Black Gold delay point. Currently, if a patron reports that another patron is viewing an inappropriate site on a library computer, SBPL staff must inform the patron to stop viewing the content as well as notify Black Gold's network administrator to block the site content in Black Gold's firewall. That process may take an inordinate amount of time depending on the network administrator's workload. The Black Gold firewall also was not designed to be a web content filter; it functions primarily as a network security gateway. Should SBPL have its own web content filtering solution, its staff would be able to directly block or allow sites very quickly.

Patrons would not be inconvenienced by this implementation. At all library branches, they would still be able to create documents and share them online, access social media, participate in online communities, upload visual materials to sites, and would still be able to participate in online gaming. Patrons will still be able to access consumer-based sites as they do now.

Aside from improved internet safety, meaningful compiled statistics (what our patrons use library internet access for), and streamlined control of its own secure internet gateway, this project will above all ensure SBPL maintains CIPA compliance.

Library technology staff are excited about this project because of its benefits and possibilities. We know it would future-proof our library's internet security and are confident this project would improve our service levels.