

LA FERIA INDEPENDENT SCHOOL DISTRICT
AGENDA ACTION SHEET

Date: September 14, 2026

Subject: Discussion of the District's Internet Safety Policy and the Children's Internet Protection Act (CIPA) Compliance and Requirements

Administrator Responsible: Alex Cespedes

Position: Chief Financial Officer

A. Purpose of Agenda Item:

☒ Information Only

☐ Action Needed

B. Authority for This Action:

☐ Local Policy

☒ Law or Rule: Children's Internet Protection Act (CIPA)

C. Strategic Objective, Goal, or Need Addressed: N/A

D. Summary: To be eligible for Schools and Libraries (E-Rate) program discounts and funding, the District (as the applicant) must certify compliance with the Children's Internet Protection Act (CIPA).

The District must certify that it is enforcing an internet safety policy that includes measures to block or filter internet access for both minors and adults to certain visual depictions.

CIPA requirements include three items:

1. Internet Safety Policy
2. Technology Protection Measure
3. Discussion/Hearing/Meeting

E. Alternatives Considered: N/A

F. Comments Received: N/A

G. Administrative Recommendation: Informational Only

H. Fiscal Impact and Cost: N/A

I. Monitoring and Reporting Timeline: Administration will continue to enforce an internet safety policy that includes a technology protection measure that protects against access by adults and minors and continue to implement technology protection measures that include capabilities such as real-time web filtering, granular policy controls, cross-device enforcement, and protections against circumvention tools like VPNs to help block or filter inappropriate content and safeguard student online activity.

TECHNOLOGY RESOURCES

CQ
(LOCAL)

Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

Availability of Access

Access to the District's technology resources, including the internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Use by Members of the Public

Access to the District's technology resources, including the internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's technology resources.

Acceptable Use

The Superintendent shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Internet Safety

The Superintendent shall develop and implement an internet safety plan to:

TECHNOLOGY RESOURCES

CQ
(LOCAL)

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

Each District computer with internet access and the District's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent.

The Superintendent shall enforce the use of such filtering devices. Upon approval from the Superintendent, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Monitored Use

Electronic mail transmissions and other use of the District's technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the internet.

Record Retention

A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management program. [See CPC]

Electronically Signed Documents

At the District's discretion, the District may make certain transactions available online, including student admissions documents,

TECHNOLOGY RESOURCES

CQ
(LOCAL)

student grade and performance information, contracts for goods and services, and employment documents.

To the extent the District offers transactions electronically, the District may accept electronic signatures in accordance with this policy.

When accepting electronically signed documents or digital signatures, the District shall comply with rules adopted by the Department of Information Resources, to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Maintain all records as required by law;
- Ensure that records are created and maintained in a secure environment;
- Maintain appropriate internal controls on the use of electronic signatures;
- Implement means of confirming transactions; and
- Train staff on related procedures as necessary.

How Palo Alto Networks Can Help Address CIPA Requirements

OVERVIEW

The Children's Internet Protection Act (CIPA), is a federal law enacted by the United States' Congress in December 2000 to address concerns about access in schools and libraries to the Internet and other information. CIPA imposes certain requirements that are tied to discounts for Internet access or for internal connections that a school or a library may receive. Further, in early 2001, the Federal Communications Commission (FCC) issued additional rules to ensure that CIPA is carried out.

CIPA REQUIREMENTS

The complete list of requirements that schools and libraries must meet in order to be CIPA compliant are defined at www.fcc.gov. Several of the key requirements are summarized below:

- **Web Filtering:** Schools and libraries subject to CIPA cannot receive the discounts offered by the "E-Rate" program (discounts that make access to the Internet affordable to schools and libraries) unless they certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors;
- **Monitoring Online Activity of Minors:** Schools subject to CIPA are required to adopt a policy to monitor online activities of minors;
- **Policy Implementation:** Schools and libraries subject to CIPA are required to adopt a policy addressing: (a) access by minors to inappropriate matter on the Internet and World Wide Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.

Schools and libraries are required to certify that they had their safety policies and technology in place before receiving E-rate funding.

HOW PALO ALTO NETWORKS ADDRESSES CIPA COMPLIANCE REQUIREMENTS

Palo Alto Networks' next-generation firewall uses three innovative technologies that allow schools and libraries to regain visibility and control over applications, users and content traversing their network. These technologies, App-ID, User-ID and Content-ID, bring the business-relevant elements of applications, users and content under policy control using a high performance firewall architecture.

- **App-ID** is a patent-pending technology that identifies and controls more than 1,200 applications irrespective of port, protocol, SSL encryption, or evasive tactic employed. App-ID can help reign in today's students who are Internet experts and are increasingly using a new class of application that can easily circumvent existing security mechanisms such as firewalls, URL filtering and proxy servers.

These applications, which include TOR, UltraSurf and PHproxy, put IT departments in a difficult position. State and Federal regulations, school board policies, community standards, and common sense dictate that schools filter applications and Internet traffic that can make its way to students' eyes and ears.

The conventional approach to solving this problem includes deploying a URL database in conjunction with a traditional network firewall, but this approach simply can't keep pace with these nimble, network-savvy applications. Today, it alone is no longer enough.

The solution is to use Palo Alto Networks and App-ID to identify the application first and foremost. Armed with the knowledge of which applications are traversing the network, IT departments can enable policies that foster education and research yet control access to the applications and content that may threaten CIPA benefits.

- **User-ID** is a technology that integrates Palo Alto Networks next-generation firewalls with Microsoft Active Directory, LDAP, eDirectory and Citrix resulting in visibility and control of applications based on users and groups – not just by IP addresses. In Citrix and terminal services environments, User-ID can associate the individual user with their network activity, enabling IT to control applications based on users that are normally obfuscated by a Citrix server. CIPA's requirement to monitor the access of minors can be addressed through a security policy that is based on user and group information from Active Directory. This association of all traffic with users and groups allows for IT staff:
 - o Regain visibility into user activities relative to the applications in use and the content they may generate.
 - o Tighten security posture by implementing policies that tie application usage to specific users and groups, as opposed to simply the IP address. Student policies can be different than Faculty, Administration, or even IT.
 - o Identify Citrix and Microsoft Terminal Services users and control their respective application usage. These tools, while allowing for multiple users to share resources are also common grounds for misuse. A single terminal server might support tens to hundreds of users/students. Again, visibility into the actual distinct users and their group membership allows for consistent policy enforcement and compliance.
- **Content-ID** is a content inspection engine that prevents a wide range of threats, blocks unauthorized file and data transfers and controls web surfing. The Internet can invite, infect, and corrupt the unsuspecting user and as such, protection against these pitfalls is critical to CIPA compliance. Palo Alto Network's next-generation firewall protects against the unauthorized disclosure, use, and dissemination of personal information regarding minors via viruses, spyware, and vulnerability exploits through the use of a uniform threat signature format and stream-based scanning architecture. The uniform signature format means that traffic is inspected only once—as opposed to the multiple scans that most other solutions must execute. Stream-based scanning means that the content scanning process begins as soon as the traffic is received.

Palo Alto Network's URL Filtering service combines an on-box dataset with a hosted service that ultimately provides access to information on over 200 million websites- ten times more than the current market leaders. This allows schools and libraries to manage Internet access to over 70 URL categories including Adult Material, Questionable, Hacking and other topics pertinent to CIPA. The dataset also maintains an up to date and comprehensive list of proxy websites in the Proxy Avoidance, and Anonymizers category, mitigating the exposure to inappropriate material accessed through this class of websites.

All of this technology runs on a high-performance, purpose-built platform based on Palo Alto Networks' Single-Pass Parallel Processing (SP3) Architecture. Unique to the SP3 Architecture, traffic is only examined once, using hardware with dedicated processing resources for security, networking, content scanning and management to provide line-rate, low-latency performance under load. Best of all, the solution complements other infrastructure technologies and can easily be deployed in virtual wire (in-line) or as a firewall.

SUMMARY

Palo Alto Networks next-generation firewalls can help schools and libraries achieve and maintain CIPA compliance while simultaneously protecting students and users from unscrupulous Internet criminals.

CIPA

Applicants must certify compliance with the Children’s Internet Protection Act (CIPA) to be eligible for Schools and Libraries (E-Rate) program discounts on Category One internet access and all Category Two services – internal connections, managed internal broadband services, and basic maintenance of internal connections. The relevant authority with responsibility for administration of the eligible school or library (the Administrative Authority) must certify that the school or library is enforcing an internet safety policy that includes measures to block or filter internet access for both minors and adults to certain visual depictions.

In general, school and library authorities must certify that: (1) they have complied with the requirements of CIPA; (2) they are undertaking actions, including any necessary procurement procedures, to comply with the requirements of CIPA; or (3) CIPA does not apply because they are receiving discounts for telecommunications services only.

Requirements

CIPA requirements include the following three items:

1. Internet Safety Policy

Schools and libraries are required to adopt and enforce an internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to use of computers with internet access by minors – harmful to minors. “Minor” is defined as any individual who is under the age of 17.

This internet safety policy must address all of the following:

- Access by minors to inappropriate matter on the internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access including “hacking” and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures designed to restrict minors’ access to materials harmful to minors.

For schools, the policy must also include monitoring the online activities of minors. As of July 1, 2012, as part of their CIPA certification, schools also certify that their internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

2. Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters internet access.

The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. For example, a library that uses internet filtering software can set up a process for disabling that software upon request of an adult user through use of a sign-in page where an adult user can affirm that he or she intends to use the computer for bona fide research or other lawful purposes.

CIPA uses the federal criminal definitions for obscenity and child pornography. The term “harmful to minors” is defined as “any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.”

Decisions about what matter is inappropriate for minors are made by the local community. E-Rate program rules specify that “[a] determination regarding matter inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination.”

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. For private schools, public notice means notice to their appropriate constituent group.

Additional meetings are not necessary – even if the policy is amended – unless those meetings are required by state or local rules or the policy itself.

Administrative Authority

The Administrative Authority for a school or library is the entity that must make the relevant certification for the purposes of CIPA. For a school, the Administrative Authority may be the school, school board, school district, local educational agency, or other authority responsible for administration of a school. For a library, the Administrative Authority may be the library, library board, or other authority with responsibility for administration of the library.

If the Administrative Authority is also the Billed Entity, the Administrative Authority certifies on the [FCC Form 486](#) (Receipt of Service Confirmation and Children’s Internet Protection Act Certification Form). If the Administrative Authority is not the Billed Entity, the Administrative Authority must complete [FCC Form 479](#) (Certification of Administrative Authority to Billed Entity of Compliance with the Children’s Internet Protection Act), and submit the FCC Form 479 to the Billed Entity. The Billed Entity then certifies on the FCC

Form 486 that it has collected duly completed FCC Forms 479. The Billed Entity does not need to collect FCC Forms 479 when the Billed Entity applies only for telecommunications services.

Determination of the First Funding Year

CIPA provides that, in the first funding year following the effective date of CIPA (April 20, 2001) in which you are “applying” for funds (see **Applying for Funds** below), you need not be fully compliant with CIPA’s requirements but can certify that you are undertaking actions to be in compliance for the next funding year. You may also make this certification in your Second Funding Year for the purposes of CIPA, if you seek a waiver due to state or local procurement rules or regulations or competitive bidding requirements. Applicants, therefore, need to determine their “first,” “second,” and “third” funding years after the effective date of CIPA (April 20, 2001) in which their school or library is “applying” for funds.

Applying for Funds

For the purposes of CIPA, a school or library that is a recipient of service is considered to have “applied” for funds in a funding year after USAC successfully processes an FCC Form 486 with at least one funding request for services that require CIPA compliance and that include that school or library.

The First Funding Year

The first funding year after Funding Year 2000 (the funding year beginning July 1, 2000) in which your school or library applies for funds (i.e., in which an FCC Form 486 is successfully processed) for Category One Internet access and/or any Category Two services is your First Funding Year for the purposes of CIPA. Once your First Funding Year is established, the next two funding years will be your second and third funding years for the purposes of CIPA. In the First Funding Year, the applicant must be in compliance with CIPA or undertaking actions to comply with CIPA in order to receive support for Category One internet access and all Category Two services.

Once the First Funding Year is established, the funding year immediately following becomes the Second Funding Year for the purposes of CIPA.

The Second Funding Year

If the school or library applies for funds for Category One internet access and/or any Category Two services in the Second Funding Year, its Administrative Authority must certify compliance with CIPA unless state or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification. A school or library so prevented can request a waiver for the Second Funding Year on FCC Form 486 or FCC Form 479, as appropriate.

The Third Funding Year

The Third Funding Year for the purposes of CIPA is the funding year immediately following the Second Funding Year. If the school or library applies for funds for Category One internet access and/or any Category Two services in the Third Funding Year, it must be compliant with CIPA.

The school or library must be compliant with CIPA for any funding year thereafter.

Certification for Undertaking Actions

Below is the appropriate certification that the Administrative Authority must make for “undertaking actions”:

“Pursuant to the Children’s Internet Protection Act, as codified at 47 U.S.C. Section 254(h) and (l), the recipient(s) of service represented in the Funding Request Number(s) on this FCC Form 486, for whom this is the first funding year in the federal universal service support mechanism for schools and libraries, is (are) undertaking such actions, including any necessary procurement procedures, to comply with the requirements of CIPA for the next funding year, but has (have) not completed all requirements of CIPA for this funding year.”

Documentation for Undertaking Actions

For a school or library to be able to make the certification quoted above, it must be able to demonstrate that action was taken by the start of services. USAC will not request this documentation as part of the FCC Form 486 filing process, but the school or library must maintain this documentation in its files for audit purposes.

An undertaken action is an action that can be documented and demonstrates that the school or library is taking steps to become compliant with the CIPA requirements. If a school or library has already provided reasonable public notice and at least one public hearing or meeting relating to an internet safety policy and technology protection measure that meets all the requirements listed above, that school or library has complied with the public notice and hearing or meeting requirements of CIPA. If a school or library has not met those conditions, the statute requires that the school or library provide the required notice and hearing or meeting.

Below are examples of documentation that could demonstrate that a school or library is undertaking actions to comply with CIPA:

- A published or circulated school or library board agenda with CIPA compliance cited as a topic
- A circulated staff meeting agenda with CIPA compliance cited as a topic
- A service provider quote requested and received by a recipient of service or Billed Entity which contains information on a technology protection measure
- A draft Request for Proposal or other procurement procedure to solicit bids for the purchase or provision of a technology protection measure
- An agenda or minutes from a meeting open to the public at which an internet safety policy was discussed
- An agenda or minutes from a public or non-public meeting of a school or library board at which procurement issues relating to the acquisition of a technology protection measure were discussed
- A memo to an administrative authority of a school or library from a staff member outlining the CIPA issues not addressed by an Acceptable Use Policy currently in place
- A memorandum or report to an administrative authority of a school or library from a staff member describing research on available technology protection measures
- A memorandum or report to an administrative authority of a school or library from a staff member that discusses and analyzes Internet safety policies in effect at other schools and libraries

This list is not meant to be exhaustive, but includes examples of how applicants can demonstrate they are undertaking actions to become compliant with the CIPA requirements.

Remember that such actions must occur before the start of services in order for discounts to be paid back to the service start date reported on the FCC Form 486. Although applicants are allowed to undertake the actions described above in order to make the required certification regarding CIPA compliance during the First Funding Year, applicants should be prepared to implement all necessary measures in order to be compliant with the CIPA requirements before services start for the Second Funding Year, unless a waiver has been granted.

Documenting CIPA Compliance

Below is a list of the documentation that will be requested to demonstrate CIPA compliance during an audit. A school or library should retain copies of the documentation for each funding year where a CIPA certification is required. Note that documents must be retained for at least 10 years after the latter of the last day of the applicable funding year or the service delivery deadline for the funding request.

- A copy of the internet safety policy
- Documentation that the school or library gave public notice and held a public hearing or meeting on the policy
 - For example, a school or library could demonstrate public notice with a copy of a website announcement for a regular school or library board meeting open to the public where the policy will be discussed, or an advertisement in a local newspaper of a county government hearing or meeting where the policy appears as an agenda item. The school or library could also demonstrate that the hearing or meeting occurred with a copy of the minutes of the hearing or meeting and the date it occurred.
 - Since 2011, entities have been required, at a minimum, to keep some record of when public notice was provided and when the hearing or meeting took place (e.g., a copy of the meeting agenda or a newspaper article announcing the hearing or meeting).
- Documentation of the adoption of the policy – for example, approval in the minutes of the hearing or meeting, or documented adoption by a school or library board
- A description of the filter
- A report or other documentation on the use of the filter
 - The documentation should show that the filter was installed and was working during the funding year.
 - For example, a school that purchased filtered internet access could archive a sampling of reports from the service provider of internet sites blocked, or bills from the service provider verifying that the filter was operational. If a school purchased its own filter, it could archive logs produced by its IT staff showing the hours the filter was engaged.
- Copies of the FCC Form 479 and/or FCC Forms 486, as applicable

Correcting CIPA Issues

Applicants are given the opportunity to correct minor errors that could result in violations of the CIPA rules before USAC institutes recovery of E-Rate program funds. Correctable errors are those that are immaterial to CIPA compliance.

Examples:

- If a school has complied in practice with its CIPA certification, but inadvertently left out one of the requirements in its written internet safety policy, the school could correct its internet safety policy as it was substantially compliant with the CIPA requirements.
- If a school or library cannot locate a record of a public notice and hearing or meeting that was held after August 2004, the school or library can correct its failure to document its public hearing or meeting by providing a public notice and holding a hearing or meeting.

These are just two CIPA issues that have been addressed by the FCC, but there may be other CIPA-related issues that can be corrected.

[USAC CIPA](#)

EXCEED CIPA COMPLIANCE WITH PALO ALTO NETWORKS

The Children's Internet Protection Act¹ is a federal law enacted by the United States Congress to address concerns around internet access in K-12 schools and libraries. To receive E-rate federal funding, schools and libraries must meet CIPA requirements.

Palo Alto Networks, the world's cybersecurity leader, enables schools to maximize student and data protection with minimal network and security resources. Palo Alto Networks Next-Generation Firewalls natively integrate multiple innovations and automation into one platform, eliminating security point products while simplifying security management and compliance. Schools rely on Palo Alto Networks to:

- Keep students safe from the latest inappropriate content and malicious sites with realtime intelligence and automated protection.
- Easily create and enforce flexible security policies for different users, applications, devices, and data.
- Simplify security management by monitoring minors' activity along with security policies, threats, and logs through a single pane of glass.
- Consistently protect data center, school, mobile, and cloud environments.
- Protect the latest digital innovations without adding more appliances or user interfaces.

Keep Students and Data Safe with a Platform Approach to Cybersecurity

Our Next-Generation Firewalls eliminate the need to buy, deploy, integrate, and separately manage multiple point products, reducing the cost and complexity of cybersecurity. Schools can choose to leverage some or all security technologies supported by standalone or virtualized firewalls to protect schools, data centers, and cloud environments. While Next-Generation Firewall features and subscriptions protect students and school operations and data in myriad ways, the table that follows provides an overview of how its capabilities contribute to CIPA compliance.

Minimum Compliance Requirements: Filtering, Visibility, and Control

Schools can meet CIPA requirements as well as keep their students, data, and operations safe with Palo Alto Networks Next-Generation Firewalls and tightly integrated innovations. At a minimum, schools should implement:

- **URL Filtering:** This subscription for Next-Generation Firewalls hosts information about hundreds of millions of websites and more than 75 URL categories, including Adult, Abused Drugs, Hacking, and other categories relevant to CIPA. URL Filtering also categorizes URLs by risk level, accounting for factors like time since registration and whether URLs are hosted on dynamic DNS platforms. URL Filtering allows schools to:
 - Block access to high-risk or inappropriate website categories.
 - Enforce Safe Search.
 - Enforce restricted YouTube access.
 - Create alerts and perform actions based on keyword searches in search results.
 - Prevent inappropriate content from appearing in minors' search results.
 - Thwart common evasion tactics, such as cached results and language translation sites.

1. Federal Communications Commission Children's Internet Protection Act, <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>.

**Palo Alto Networks Next-Generation Firewall Capabilities That Contribute to
CIPA Compliance Across Endpoint, Network, and Cloud Environments**

CIPA Requirement	Minimum Requirements for CIPA Compliance					Best Practices to Reduce Risk					
	URL Filtering*	User Identification	Application Identification	SSL Decryption	Threat Prevention*	Zero-Day Malware Prevention	Remote Security*	Data Filtering Profiles	Zero Trust Network Segmentation	Credential Theft Prevention	DNS Security*
Web filtering to block images that are obscene, contain child pornography, or are harmful to minors	✓	✓	✓	✓		✓	✓				
Online activity monitoring of minors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Prevention of access by minors to inappropriate material on the internet	✓	✓	✓	✓			✓	✓			
Assurance of minors' safety when using email, chat rooms, etc.	✓	✓	✓	✓			✓				
Blocking of unauthorized access, hacking, and other unlawful activities by minors online	✓	✓	✓	✓	✓		✓	✓		✓	✓
Prevention of disclosure, dissemination, or use of minors' personal information		✓	✓	✓	✓			✓		✓	✓
Restricted access to materials harmful to minors	✓	✓	✓	✓	✓			✓		✓	✓

*Capability available by subscription

- **User identification (User-ID™ technology):** This standard feature on every Next-Generation Firewall enables schools to create and view policies, reporting, and forensics based on users and groups—not IP addresses. Administrators can associate students with their network activity, gaining insight that can meet monitoring requirements, help refine security and network usage policies, and reduce incident response times. Next-Generation Firewalls leverage user information from a wide range of repositories, including LDAP services such as Microsoft Active Directory®, Microsoft Exchange, and Novell eDirectory; XML APIs; and syslog messages from wireless LAN controllers and other devices.
- **Application identification (App-ID™ technology):** This patented technology identifies and controls more than 3,000 applications, irrespective of port, protocol, SSL encryption, or evasive tactics. Schools can foster education and research while controlling access to applications and content harmful to minors. Working in conjunction with URL Filtering and User-ID, App-ID enables schools and districts to:
 - Allow, deny, or even bandwidth-limit applications for an entire school, by user, or by group.
 - Enforce granular usage policies—for example, allow certain social media applications on school-owned computers while denying the chat feature, or allow file downloads while denying file uploads to file sharing and storage apps.
 - Identify and block proxy technologies, such as Tor, Ultrasurf, and PHPProxy, designed to circumvent port-and-protocol firewalls, web filtering technologies, and proxy servers.

- **SSL Decryption:** All Palo Alto Networks firewalls perform decryption, improving visibility into potential threats while eliminating the management overhead and performance impact of separate decryption appliances. Schools can:
 - Decide which inbound and outbound traffic to decrypt based on URL categories, source users, and source/destination IP addresses.
 - Decrypt traffic in virtual wire, Layer 2, or Layer 3 mode, and even decrypt HTTP/2 streams, maintaining performance benefits instead of downgrading sessions to HTTP/1.1.
 - Inspect decrypted traffic for threats and apply security policies.
 - Create a copy of decrypted traffic and send it to a traffic collection tool for archiving and analysis using the Decryption Port Mirror capability.
- **Threat Prevention:** This subscription for Next-Generation Firewalls eliminates evasive threats at every stage of an attack, preventing exploits from reaching devices, disrupting command-and-control traffic, and enforcing IPS protections across all ports and protocols.

Exceed Compliance with Best Practices

Schools should strongly consider configuring these capabilities to stop new and evolving threats from traversing the network, exfiltrating sensitive data, or allowing inappropriate content to find its way to minors. With thousands of new websites created every day, the only way to prevent threats or inappropriate content from reaching schools and students is realtime, automated protection. Some school districts monitor school-owned devices for CIPA compliance even after the devices have left the school network, while others only monitor within school boundaries. Either way, schools must extend security policies to school-owned devices, including 1:1 devices. Palo Alto Networks Next-Generation Firewalls can help in multiple ways:

- **Zero-day threat prevention**, enabled by WildFire® malware prevention service, automatically detects and stops unknown threats that would harm minors or steal data. Realtime data from the world's largest threat intelligence sharing community rapidly identifies unknown threats, and the service automatically delivers protections in as few as five minutes after a threat is discovered anywhere in the world. WildFire works with URL Filtering to automatically block brand-new inappropriate or malicious URLs.
- **Remote security**, enabled through a subscription to GlobalProtect™ network security for endpoints or Prisma™ Access, secures mobile device and branch location traffic flows to data center and cloud applications with IPsec/SSL VPN tunnels. It can apply the same, consistent security policies to school-owned devices, including laptops, tablets, and more.
- **Data filtering profiles** prevent sensitive information, such as credit card and Social Security numbers, from leaving a protected network. You can filter keywords that signal harmful or threatening content for certain applications or file types.
- **Zero Trust network segmentation** protects sensitive data and traffic flows within your organization, ensuring valid users have access to the resources they need while denying all others. It also prevents malware from spreading from untrusted networks to critical applications, such as from school wireless networks to the data center. Network segmentation works in conjunction with URL Filtering, App-ID, User-ID, data filtering, and remote device security to consistently secure your most sensitive data and applications.
- **Credential theft prevention** stops your users from submitting passwords to unknown sites, works with URL Filtering to block access to known phishing sites, and stops hackers from using stolen credentials to gain access to your systems.
- **DNS Security service** applies predictive analytics, machine learning, and automation to block misuse and attacks that use DNS, and eliminates the need for independent tools.

More Information

For more details about Palo Alto Networks technology and how we secure education, see these resources:

- Read about [our work with K-12 schools](#).
- Learn about [our industry-leading Next-Generation Firewalls](#).
- Understand how [our offerings support the E-rate Program](#).
- See how [our Next-Generation Firewalls decrypt web traffic in a K-12 environment](#).



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. exceed-cipa-compliance-ds-103119