The CIPA Act

CIPA-Children's Internet Protection Act (CIPA) is a federal law to address concerns about access in schools and libraries to the Internet and other information, enacted by the United States’ Congress in 2000. CIPA requires that schools and libraries which receive funding under the E-Rate program must have an Internet Safety Policy in place that addresses the safety and security of minors online.

The CIPA act was revised to incorporate the E-rate provisions of 'Protecting Children in the 21st Century Act' enacted in 2008. The new Internet Safety Policy requirement becomes effective for FY 2012, the E-rate funding year beginning July 1, 20124. The new rules require schools to amend their existing Internet Safety Policy if it does not already comply with the new standards4.
CIPA Requirements

As per the official guide by Federal Communications Commission - FCC for CIPA requirements, it includes the following three items:

**Technology Protection Measure**

The protection measures must block or filter Internet access to pictures that are:
- a) obscene;
- b) child pornography;
- c) harmful to minors (for computers that are accessed by minors).

It may be disabled/modified for adults engaged in educational, research or other lawful purposes. It must also include monitoring the online activities of minors, for schools. Documentation of the technology protection measure (e.g., filter logs & reports) must be retained for at least five years.

**Internet Safety Policy**

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- a) Access by minors to inappropriate matter on the Internet;
- 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) Measures restricting minors’ access to materials harmful to them.

**Public notice of and public meeting or hearing on the Internet safety policy**

The authority with responsibility for administration of the school must provide reasonable public notice and hold at least one public hearing to address a proposed technology protection measure and Internet safety policy. Unless local or state laws require you to do so, you will not be required to hold new public hearings to amend your policy to comply with the new CIPA regulations. Retain documentation of public notice (e.g., flyer or newspaper notice) and of the hearing or meeting (e.g., agenda and minutes) for at least five years.
As mentioned above, the CIPA act was revised to incorporate the E-rate provisions of the ‘Protecting Children in the 21st Century Act’ enacted in 2008. The most important aspect of the new Order (FCC 11-125) is that Schools and libraries subject to CIPA are required to make a statement that they are "educating minors about appropriate online behaviour, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response".

The new rule also adds that at times of audit, schools must have documentation to support their CIPA compliance. Failure to provide documentation may result in the loss of continued E-Rate funding and/or obligate the school to reimburse the full costs for Internet services for any fiscal year in which the school was found to be non-compliant.

Cyberoam enables schools/libraries to comply with CIPA, with multiple security features available over a single appliance. It allows administrators to enforce Internet safety policies that block and filter Internet access in accordance with CIPA requirements, critical in enabling schools and libraries to qualify and continue receiving government funding from the E-Rate Program. Cyberoam Next Generation Firewall (NGFW) appliance ensures CIPA compliance by offering inbuilt CIPA compliance policy settings. Cyberoam’s comprehensive security enables schools/libraries to

- Control Indiscriminate Surfing & Blocks Objectionable online content
- Ensure Safety and security of minors when using electronic communications
- Prevent disclosure of minors’ personal information and illegal intrusions
- Get Layer 8 Identity-based security – User based controls and monitoring even in shared computing environment
- Get detailed Logging and Reporting
Control Indiscriminate Surfing & Blocks
Objectionable online content
Preventing access by minors to inappropriate matter on the Internet and implementing measures to restrict minors’ access to materials harmful to them, is a key aspect schools/libraries need to achieve in order to comply with CIPA.

Cyberoam’s Web & Content Filtering prevents indiscriminate surfing by blocking access to inappropriate websites with an automated web categorization engine – ‘WebCat’ that has one of the most comprehensive URL database of 44 million+ URLs in 82+ categories including categories of websites like adult, porn, nudity, violence, proxy. It blocks and inspects HTTPS sites & Google Cached pages, and even controls Google search by specific keywords and enforce ‘Safe Search’ feature of Search Engines to filter inappropriate keywords. It also enables you to educate students/users healthy-usage policy by providing customized messages on blocked websites. Administrators have the ability to add websites to the blocked website list, customizing Cyberoam’s security to meet their school’s requirements.

With Cyberoam, network administrators can control access to web mail, chat applications by blocking access or blocking file uploads.

Moreover, Cyberoam helps block malware, spam at gateway level with its Gateway Anti Virus, Anti-Spam features that scans HTTP, FTP, SMTP, POP3, HTTPS, IMAP and IM traffic. Cyberoam protects schools/libraries from data leakage and loss occurring with data transfer over email, web and applications and gives the administrator complete control access to school records or other applications. Cyberoam’s Instant Messaging Archiving and Control feature controls who chats with whom, besides controlling file transfer, voice and video chats over Instant Messengers, preventing data leakage, phishing, malware, viruses, Trojans, worms, botnets and other malicious attacks over instant messaging. It offers granular logs and reports, providing visibility and archiving facility to help meet CIPA compliance requirements.

Cyberoam also offers comprehensive network protection from outbound and inbound spam, using its Gateway Anti-Spam (Inbound/Outbound) that protects schools/libraries from the hazardous menace of spam, using the Recurrent Pattern Detection (RPD™) technology, enabling virus outbreak detection providing zero-hour protection.

Ensure Safety and security of minors when using electronic communications
Yet another challenge schools/libraries face while adhering to CIPA is the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.

With Cyberoam, network administrators can control access to web mail, chat applications by blocking access or blocking file uploads.

Moreover, Cyberoam helps block malware, spam at gateway level with its Gateway Anti Virus, Anti-Spam features that scans HTTP, FTP, SMTP, POP3, HTTPS, IMAP and IM traffic. Cyberoam protects schools/libraries from data leakage and loss occurring with data transfer over email, web and applications and gives the administrator complete control access to school records or other applications. Cyberoam’s Instant Messaging Archiving and Control feature controls who chats with whom, besides controlling file transfer, voice and video chats over Instant Messengers, preventing data leakage, phishing, malware, viruses, Trojans, worms, botnets and other malicious attacks over instant messaging. It offers granular logs and reports, providing visibility and archiving facility to help meet CIPA compliance requirements.

Cyberoam also offers comprehensive network protection from outbound and inbound spam, using its Gateway Anti-Spam (Inbound/Outbound) that protects schools/libraries from the hazardous menace of spam, using the Recurrent Pattern Detection (RPD™) technology, enabling virus outbreak detection providing zero-hour protection.
Prevent disclosure of minors’ personal information and illegal intrusions
Avoiding unauthorized access, including so-called “hacking,” and other unlawful activities by minor’s online and preventing unauthorized disclosure, use, and dissemination of personal information regarding minors is one of the major requirements schools/libraries need to adhere to for CIPA compliance.

Cyberoam’s IPS and on-appliance Web Application Firewall features ensure security from intrusion attacks and hacking attempts hackers that exploit web-application vulnerabilities in institutes’ data centers. Schools today use a wide array of web applications including Student Information System, Library -Textbook Management, Email (both students and faculty/staff) - Google Apps, Donor Management, Work-Study Management – Salesforce, Visitor Management, and so on. Cyberoam’s On-appliance Web Application Firewall, protects websites and web servers from hackers and also prevents hackers from exploiting Web-Application Vulnerabilities (like OWASP TOP10).

Apart from these, Cyberoam offers comprehensive network protection from Virus and Spyware, using its Gateway Anti-Virus and Anti-Spyware. It conducts bi-directional scanning for both Web & Email, preventing intrusion attempts (including hacking and bots), malware, Trojans, DoS and DDoS attacks, malicious code transmission, backdoor activity and blended threats. Cyberoam offers protection from intrusion attacks, unauthorized access with its Intrusion Prevention System, which protects servers (database server, email server, etc.). It enables administrators to apply user or group Identity-based IPS policies. It has a broadest security cover with 3500+ signatures.

Get Layer 8 Identity-based security – User based controls and monitoring even in shared computing environment
In most educational institutes, students share the same computer creating a shared computing environment. Lack of knowledge on who is doing what and no real-time visibility into user activity in such networks, makes investigative and forensic analysis difficult in case of wrongful usage of network. Adding to this, monitoring the online activities of minors is a very important rule for schools/libraries that need to adhere to while complying with CIPA. Hence administrators can’t ignore monitoring and tracking user activity in their networks.

Cyberoam with its Layer 8 security enables network administrators to get complete and centralized monitoring of student activity in real-time, allowing administrators to identify the students instantly. Cyberoam NGFW works on a unique Layer 8 Technology that treats the 8th Layer as the Human Layer in the network protocol stack. This basically adds human identity to the entire security process. Cyberoam identifies each user in the network by a username instead of just an IP address allowing the administrator to identify user responsible for unproductive surfing. Further to this, the authentication can be done on a combination of username, IP Address and MAC Address. It gives real-time details of ‘who is doing what’ in the network, allowing immediate corrective security action. It supports high levels of security and data confidentiality while meeting the requirements of regulatory compliance. Cyberoam Application Visibility & Control feature offers complete visibility on which applications are being accessed within the network and by which user (student/faculty).
Get detailed Logging and Reporting
Documentation of user activity and the technology protection measure including filter logs and reports is crucial for schools that want to stay CIPA compliant.

Cyberoam offers Layer 8 Identity-based reporting, offering visibility into the institution’s surfing trends, bandwidth and system utilization, Internet usage in addition to intrusion alerts and more. It offers 1200+ reports that give real-time visibility into user and network activities, besides allowing security management, compliance management for CIPA and more, along with forensic analysis capability. Cyberoam offers real-time graphical reporting with dashboards and drill-down reports to the third level with identity-based information related to network events and user activity allowing institutes to take quick remedial actions.

Cyberoam-Comprehensive Network Security

In addition to ensuring that schools and libraries comply with CIPA requirements, Cyberoam offers complete protection from both internal and external threats and more. Cyberoam offers a complete set of security features like stateful inspection Firewall, Virtual Private Network (VPN), Gateway Anti-virus/Anti-Spyware, Gateway Anti-spam, Intrusion Prevention System (IPS), Content Filtering, Web Application Firewall, on-appliance reporting, Bandwidth Management, Multiple Link Management and more.

Network Security even in Wi-Fi environments
With increasing use of Wi-Fi in schools and libraries and students, network security over Wi-Fi has become must. Cyberoam Wi-Fi security appliances protect schools and libraries with public Wi-Fi access, from intrusions, identity theft through MAC spoofing, DoS attacks and malware entry. They offer Layer 8 Identity-based security, providing high levels of security with flexibility in wireless LANs. The appliances support 802.11n/b/g wireless standards. They combine the features of a router and Cyberoam’s complete set of NGFW features, offering completely secure networks to its users.

Centralized Security Management & Monitoring for multiple branches
For educational institutes having multiple centers or sites, Cyberoam offers administrators the ability to centrally manage security and visibility using a Cyberoam Central Console (CCC) and Cyberoam iView-logging and reporting solutions. CCC enables educational institutions to centrally manage updates and security policies in real-time across multiple branches at remote locations, minimizing response time. CCC helps in quick monitoring and action and offers flexibility in sorting appliance views on the dashboard and also allows setting email alerts for individual or group of Cyberoam NGFW appliances based on parameters like expiry of subscription modules, excess disk usage, IPS and virus threat counts, unhealthy surfing hits and more. Cyberoam iView offers centralized logging and reporting of network and user activity over multiple devices across distributed locations/branches, providing real-time and historical information of security events to network administrators. Available as an open source solution and as a dedicated appliance, it offers intelligent logging and reporting with Layer 8 Identity-based visibility.
Conclusion

Cyberoam’s unique Identity-based security enables schools and libraries to enforce an Internet safety policy that blocks and filters Internet access in accordance with CIPA requirements using its powerful content filtering, and comprehensive security features. It also offers complete visibility into individual users, allowing schools and libraries to protect students while securing the institution from varied complex, legal and CIPA compliance issues. In addition, it plays a central role in securing E-Rate funding for their Internet access and Internet connection investments.

Learn More
Visit www.cyberoam.com or contact us at sales@cyberoam.com for more information. Cyberoam solutions will help you achieve CIPA compliance while protecting students and faculty from exposure to inappropriate content.

2 http://networkmaine.net/enrollment/PDF/CIPA_K12.pdf
4 http://networkmaine.net/enrollment/PDF/CIPA_K12.pdf
5 http://networkmaine.net/enrollment/PDF/CIPA_K12.pdf

Cyberoam Awards & Certifications: