1. What is CIPA?

Answer:
Please see https://www.usac.org/e-rate/applicant-process/starting-services/cipa/ for details.

The Children's Internet Protection Act (CIPA) requires that schools and libraries implement Internet safety policies in order to receive federal technology funding such as E-Rate discounts. This Internet safety policy must include filtering or another "technology protection measure" that blocks access to "visual depictions" of obscene material, child pornography and material that is "harmful to minors".

2. How does it work?

Answer: The IBOSS SWG provides web and ftp filtering through a sidescan technology that does not depend on the use of proxy servers and scales well for use in very large networks. Classification of sites is performed through the use of neural net analysis, review of linked content, and human review. Updated filter lists are downloaded daily.

3. What must my school system or library do in order to be "CIPA Compliant"?

Answer: The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed Technology Protection Measure and Internet Safety Policy.

1) Implement a "Technology Protection Measure" (e.g. filtering software)
    a) A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect 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. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors by means determined by the local system.

2) Design and implement an "Internet Safety Policy"

   The Internet Safety Policy must address the following issues:

   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) Measures designed to restrict minors' access to materials harmful to minors.

   f) Note: beginning July 1, 2012, when schools certify their compliance with CIPA, they will also be certifying 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.

3) Public Notice and Hearing

4. **How does the ASA Content Filtering Solution address CIPA Compliance?**

Answer: In order for a school system or library to be "CIPA Compliant" the steps explained by CIPA and briefly highlighted above must be followed. Simply utilizing ASA's content filtering option does NOT make your organization "CIPA Compliant".

Any ASA client for no additional charge may use the ASA content filtering service as the "technology protection measure" defined in the CIPA. The decision to use or not use ASA's filtering solution is entirely at the discretion of the individual school system or library.

5. **Can I use the ASA solution in conjunction with my own solution?**

Answer: Yes. Many ASA clients have expressed interest in maintaining their existing content filtering solution while also using our system. It would be possible, for example, to keep some existing systems for their reporting and monitoring capabilities but cancel an update subscription. In this scenario the legacy system would catch, classify, filter, and report all old sites that are blocked, while the ASA solution would filter all new sites.

6. **How can I specify what types of sites will be filtered for my individual system?**

Answer: Each school system can develop their own profile of categories that they wish to block. School systems also have the option to manage their own profiles.

For more details contact the ASA helpdesk.

7. What if a site is NOT filtered that should be?

Answer: The IBOSS SWG filtering software automatically reviews unclassified sites and updates the filtering lists. This review and update process can take up to 72 hours in some cases.

If a site is not filtered within 72 hours of initial access, technology coordinators, superintendents, or network managers can submit a site manually via the following URL:

http://resources.iboss.com/support/url_submission.html