



Compliance with CIPA, Version 2.1: **The E-Rate Internet Filtering Mandate**

Purpose for and Contents of this Document

This document is intended to help schools understand the requirements of the Children's Internet Protection Act (CIPA) as it applies to E-Rate recipients, by updating the January 2001 Filtering Compliance memo provided to members of the Consortium on School Networking (CoSN). *This is only a guide and should not be understood as the definitive interpretation of this law or as legal advice.*

The first memo http://www.cosn.org/members/cipa_compliance_documentation.pdf outlined CoSN's understanding of the requirements Congress imposed on schools and libraries receiving certain types of E-Rate, Department of Education, and Institute for Museum and Library Services funding for computers with Internet access with the passage of the Children's Internet Protection Act (CIPA), which became law at the very end of 2000. It also attempted to help schools and libraries understand what kinds of rules might be promulgated by the federal agencies responsible for such funding.

On April 5, 2001, the Federal Communications Commission released a Report & Order (part of Docket Number 96-45), providing schools and libraries receiving E-Rate discounts with additional compliance guidance. In addition, the Schools & Libraries Division of the Universal Service Administrative Company, which implements the E-Rate, released guidance on a pressing Program Year 4 question and indicated that it will be issuing additional guidance in the future.

The Department of Education and the Institute for Museum and Library Services have not promulgated any rules interpreting CIPA, nor have they indicated plans to do so. However, both the Department of Education and IMLS have indicated that CIPA does not impose *any* requirements on current grantees. The Department of Education has indicated that it expects to require grantees in the next fiscal year (beginning October 1, 2001) to comply with CIPA, while the IMLS has suggested compliance will be required beginning in October 2002.

This memo will focus exclusively on the CIPA requirements applying to E-Rate recipients. The memo will explain:

- Overview of the new FCC Rules & rulemaking process;
- Who must comply with CIPA;
- The compliance certification process;
- The time frame for compliance;
- The requirements with respect to filtering technology and Internet Safety Policies ;
- When filters may be disabled and for whom;
- Monitoring student Internet use;
- Penalties for failure to comply; and
- The implications of ALA and ACLU lawsuits challenging CIPA s library provisions.

Overview of the FCC CIPA Rulemaking Process

The FCC conducted a rulemaking process on CIPA during the first few months of 2001. As a result, they issued a Report and Order on April 5, 2001. Sixty parties filed comments on the proposed rules, and twenty filed reply comments. The parties filing comments or reply comments ranged from individual citizens and librarians from local libraries and state library associations, to national civil liberties, library, and education associations, conservative anti-pornography groups, and the trade association representing the smaller filtering products and services. Commenters requested clarification and made arguments for particular interpretations of the law in a number of areas, including:

- Whether E-Rate Program Year 4 or 5 should be considered the first program year following CIPA s passage;
- What software, if any, meets the requirements of CIPA;
- The meaning of bona fide research ;
- What constitutes monitoring students Internet use;
- How to determine whether filtering was effective or accurate;
- Whether administrative computers not available to members of the public were subject to CIPA s requirements;
- How to manage certification when an entity receives E-Rate funding for a consortium whose members may not all be public schools, schools, or school libraries, and thus subject to CIPA requirements.

Who Must Comply with CIPA

- Any school that receives discounted rates for Internet access, Internet service or internal connections under the E-Rate program ***must comply*** with CIPA.
- If a school receives only telecommunications services through E-Rate, it ***does not need to comply*** with CIPA.
- If a school receives no E-Rate funding, it ***does not need to comply*** with these rules.¹

¹ Schools may still have to comply with CIPA if they receive funds under ESEA. The Department of Education has not yet issued CIPA guidance. Please check www.cosn.org for additional information as it becomes available.

Time Frame for Compliance: Part 1

CIPA applies to funds received during E-Rate Program Year Four, which begins July 1, 2001. Schools do not have to *complete* the certification requirements above until October 28, 2001.² However, the funds will not be released until the recipient has certified as above. The FCC and Schools & Libraries Division have indicated that funds for Year 4 may be paid retroactively as far back as July 1 if certification is made by October 27, as long as the entity is taking actions to comply with CIPA *at the time that it actually receives these services*. (Corrected Report and Order, para. 15.; emphasis in original.)

The Schools & Libraries Division (SLD) further clarified the need for schools to be undertaking actions to comply with CIPA *before July 1, 2001*. According to the SLD's Specific Guidance for Year 4 Undertaking Actions Certification, in order to receive E-Rate support, schools must have undertaken some action toward compliance with CIPA in order to receive E-Rate support, schools must have undertaken some action toward compliance with CIPA *by the Service Start Date*. If service begins at the start of the new E-Rate Funding Year, that date is July 1, 2001.

A school could undertake and document the following types of actions in order to meet this SLD requirement:

- 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 of an RFP 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 nonpublic 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 Accessible Use Policy currently in place.
- A memo or report to an administrative authority of a school or library from a staff member describing research on available Technology Protection Measures.
- A memo or report to an administrative authority of a school or library from a staff member which discusses and analyzes Internet Safety Policies in effect at other schools and libraries.

CIPA also requires school authorities to hold a public meeting or hearing to discuss the adoption of an Internet Safety Policy that includes use of filtering technology. If a

² Technically, the statutory deadline is October 28, 2001. However, that is a Sunday, and the FCC has indicated that certifications postmarked on October 29 will be considered untimely. This renders the effective date for compliance October 27, 2001.

school's current Internet Safety Policy (more commonly known as an Acceptable Use Policy) includes all of the CIPA-required elements (described below), *and* was developed with at least one public meeting, no further action is necessary in order to comply. Specifically, the FCC indicated at para. 51 of the corrected Report and Order:

If an entity has already provided reasonable public notice and at least one public hearing or meeting related to an Internet safety policy and technology protection measure that meets the requirement[s] of [CIPA], then we conclude that the entity has already complied with the public notice and hearing requirements of CIPA. If an entity has not met those conditions, we conclude that the statute requires that the entity provide the required notice, and hearing or meeting.

Special note for private schools: Congress appeared to limit the public meeting requirements for private schools to those members of the public with a relationship to the school. However, the FCC found that *all* schools eligible for E-Rate funding fall within the definitions used by Congress in the section requiring public hearings or meetings with public notice. Consequently CIPA appears to require private schools to hold an open public meeting or hearing on its Internet safety policy.

Time Frame for Compliance: Part 2

The SLD is presently considering how to most effectively manage the certification process for E-Rate Program Year Four recipients. Schools will likely be eligible to make a certification shortly after Funding Commitment Decision Letters (FCDLs) go out, and certainly will be able to do so by July 1, 2001.

For schools that are not presently compliant with all of the elements of CIPA, there is a phase in period during which schools may certify that they are in the process of becoming compliant, but are not presently compliant. During Program Year Four, many schools are likely to certify that they are undertaking steps toward becoming compliant.

During E-Rate Program Year Five, some one-year waivers will be available for schools that are legally restrained by state or local bidding requirements, if they cannot become CIPA compliant by the end of Program Year Four. By E-Rate Program Year 6 (July 1, 2003), all applicants receiving internal connections and Internet access discounts will need to comply with CIPA.

New applicants beginning in E-Rate Program Year 5 or later are subject to the certification requirements current applicants must meet this year. The language of the CIPA statute refers to requirements for the first program year following passage [of CIPA] and creates parallel requirements for new applicants in future years. This means, for example, that all new E-Rate applicants will have until October of their first year participating in the E-Rate program, to certify compliance with CIPA.

School Entity Certification Requirements

In order to ensure the flow of Program Year 4 funds, schools must make one of three possible CIPA compliance certification options on a revised FCC Form 486:

1. *Currently Compliant with CIPA*
The recipient(s) of service represented in the Funding Request Number(s) on this Form 486 has (have) complied with the requirements of the Children s Internet Protection Act, as codified at 47 U.S.C./254(h) and (l).

2. *Undertaking Action to Become Compliant with CIPA*
Pursuant to the Children s Internet Protection Act, as codified at 47 U.S.C./254(h) and (l), the recipient(s) of service represented in the Funding Request Number(s) on this Form 486 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.

3. *Not Required to Comply with CIPA*
The Children s Internet Protection Act, as codified at 47 U.S.C./254(h) and (l), does not apply because the recipient(s) of service represented in the Funding Request Number(s) on this Form 486 is (are) receiving discount services only for telecommunications services.

Consortium Certification Requirements

If a school receives E-Rate funding as part of a consortium application individual consortium members complete the new Form 479. Instead of filing Form 479 with the Schools & Libraries Division, Forms 479 are filed with the Billed Entity, which files a Form 486 on behalf of members of the consortium. State network applicants will most likely be treated as consortia for the purposes of certification, although the FCC has not been completely clear about this. CoSN is seeking further guidance on the application of CIPA to state networks and will post that clarification as soon as possible. In the meantime, state network applicants should contact the USAC with questions about their specific circumstances.

The statements schools choose from on Form 479 are substantially similar to the certifications on Form 479. The Billed Entity then files a Form 486 on behalf of the consortium. The Billed Entity must make one of two additional certifications:

1. I certify as the Billed Entity for the consortium that I have collected duly completed and signed certifications from all eligible members of the consortium.

2. I certify as the Billed Entity for the consortium that the only services received under the universal service support mechanism by eligible members of the consortium are telecommunications services, and therefore the requirements of the Children s Internet Protection Act, as codified at 47 U.S.C./254(h) and (l), do not apply.

The Billed Entity only certifies that it has received signed Forms 479 from all of its members; it is not liable for determining the actual compliance of those members.

Requirements of the Internet Safety Policy

The CIPA statute requires schools to use filtering & blocking technology and to implement a set of substantive policy decisions related to Internet access, calling both requirements an Internet Safety Policy. This causes some confusion, particularly as the requirements are located in different parts of the statute.

With regard to the policy elements of the Internet Safety Policy, CIPA requires that schools address all of the following specific elements:

- Access by minors to inappropriate material 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; (i.e. Instant Message services)
- Unauthorized access, including so-called hacking and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
- Measures designed to restrict minors access to materials harmful to minors;
- A plan to monitor minors use of the Internet in school.

In addition, the Internet Safety Policy must require the installation and use of filtering software or services on **all** computers with access to the Internet. When **minors** are using the Internet, access to visual depictions **must** be blocked or filtered if they are:

- obscene,
- child pornography, or
- harmful to minors

When **adults** are using the Internet, only material which is obscene or child pornography must be filtered or blocked.

Selecting and Disabling the Filters

The FCC declined to respond the request of several commenters to identify which filtering products, if any, complied with CIPA. Instead, it specifically found that local communities are the correct authorities to make this decision.

Schools receiving covered E-Rate support **cannot disable** the computers when **minors** are using them, even with parental or teacher permission and supervision.

Appropriate school staff **may disable** filters for **adults** using school computers for bona fide research purposes. The FCC also declined to further define *bona fide research* or *other lawful purposes*. Specifically, the FCC said:

We decline to promulgate rules mandating how entities should implement these provisions. Federally-imposed rules directing school and library staff when to disable technology protection measures would likely be overbroad and imprecise, potentially chilling speech, or otherwise confusing schools and libraries about the requirements of the statute. *We leave such determinations to the local communities, whom we believe to be most knowledgeable about the varying circumstances of schools and libraries in those communities.* (Corrected Report & Order, para. 53, emphasis added.)

Monitoring Student Internet Use

The process for monitoring students' Internet use was also left to local decisionmaking. The final language of the CIPA law was very clear that electronic monitoring and data collection is not required for schools to comply with the monitoring requirement. However, it is also clear that schools preferring to use technology to monitor students' online activities may do so.

Penalties for Noncompliance & Failure to Certify

Schools that *knowingly* fail to comply and certify compliance with CIPA lose eligibility for federal support and are responsible for paying the full price of applicable E-rate eligible services. Billed Entities that knowingly fail to certify will also render the entire consortium ineligible. Specifically, the FCC Rule (47 CFR/54.520(d)(1)) indicates:

A school or library [or billed entity] that *knowingly* fails to submit certifications as required by this section, shall not be eligible for discount services under the federal universal service support mechanism for schools and libraries until such certifications are submitted.

47 CFR/54.520(e)(1) further indicates:

A school or library [or consortium] that *knowingly* fails to ensure the use of computers in accordance with the certifications required by this section, must reimburse any funds and discounts received under the federal universal service support mechanism for schools and libraries for the period in which there was noncompliance.

Entities reestablishing compliance will become eligible for discounts when they certify compliance.

Lawsuit Challenging CIPA

There are no challenges at this time to the school-based requirements of CIPA.

Both the ACLU and the American Library Association (ALA) have filed lawsuits challenging CIPA's constitutionality. Both the ACLU and the ALA lawsuits focus on the impact of CIPA on *public libraries*. While it is remotely possible that the court will decide to strike down the whole statute, we believe that it is highly unlikely.

Therefore, school entities should not assume that the ACLU and ALA challenges will have an impact on schools or school libraries receiving funding from sources covered by CIPA and should take the necessary steps to comply with the CIPA requirements.