Children's Internet Protection Act (CIPA) Primer for PA Libraries

Presented by:
Julie Tritt Schell, PA E-rate Coordinator
jtschell@comcast.net
www.e-ratepa.org
December 2021

Topics

- History of CIPA
- When Does CIPA Apply?
- What is Required
  - Internet Safety Policy
  - Filter
    - What must be filtered?
    - When can a filter be disabled?
    - What if a filter fails?
  - Public Hearing
- Who Certifies CIPA Compliance and How?
- What if You’re Not Compliant?
- How to Prepare for E-rate or ECF Audit
- Your Questions, Answered
- Resources

History of CIPA

- The 1996 Communications Decency Act (CDA) was the first attempt by Congress to regulate content on the Internet
  - Because its overly broad and vague language infringed on First Amendment rights, the Supreme Court found the CDA unconstitutional in 1997
- In Dec 2001, Congress passed the Children's Internet Protection Act (CIPA)
  - More narrowly focused on protecting children from obscene material on the Internet
- ALA filed suit, claiming that like the CDA before it, CIPA infringed on the First Amendment rights of library patrons
  - In June 2003, US Supreme Court found CIPA constitutional
  - Libraries and schools must be CIPA compliant or "undertaking actions" in the first year after FY 2000 that they receive E-rate funds
    - If undertaking actions, must be fully CIPA compliant in the next funding year
- In 2008, Congress passed the Protecting Children in the 21st Century Act which added statutory language to CIPA requiring schools to educate minors "On appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and [on] cyberbullying awareness and response."
  - *Schools* (only) were required to be in compliance by July 2012
  - This act does not apply to libraries

When Does CIPA Apply?

- If a library receives E-rate funding for Internet access or internal connections

- or -

- If a library receives ECF funding for Internet access

- or -

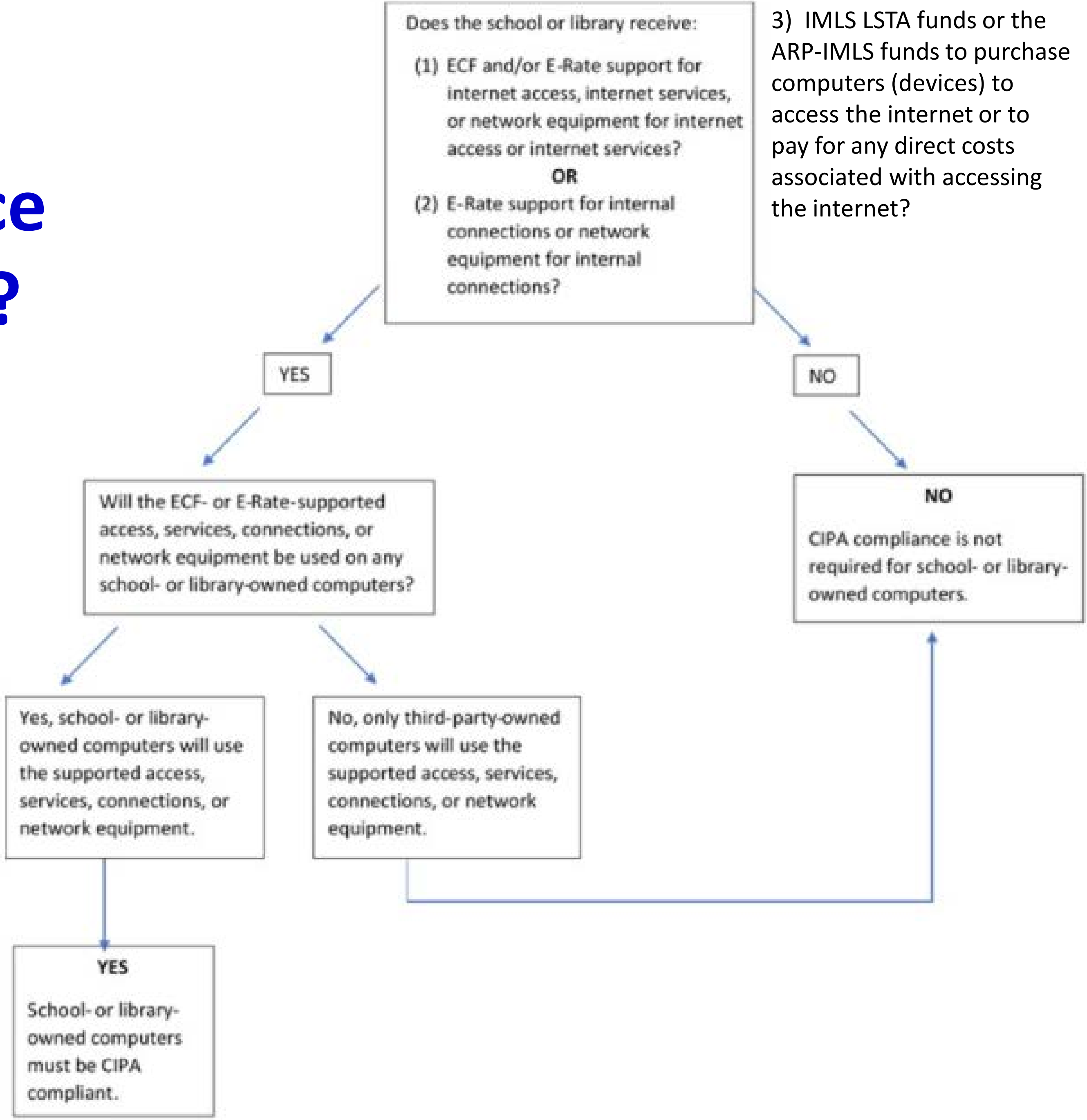
- If a library uses IMLS federal funds to purchase Internet access, or computers/devices that will access the Internet

… CIPA applies, even if the library itself is not the applicant, but is receiving E-rate, ECF or IMLS funding (noted above) via another organization, such as a consortium.

…CIPA is triggered by ownership of a device, not the location where the device is being used.

Note: CIPA compliance, as discussed in this presentation, describes the requirements for libraries using most federal funds for internet services and connected devices. Being CIPA compliant under these federal funding programs also meets Pennsylvania's CIPA-specific requirements (Act of Nov 30, 2004, P.L. 1556, No. 197 Cl. 35).

Is CIPA Compliance Required?



Does the school or library receive:

(1) ECF and/or E-Rate support for internet access, internet services, or network equipment for internet access or internet services?

OR

(2) E-Rate support for internal connections or network equipment for internal connections?

3) IMLS LSTA funds or the ARP-IMLS funds to purchase computers (devices) to access the internet or to pay for any direct costs associated with accessing the internet?

YES

Will the ECF- or E-Rate-supported access, services, connections, or network equipment be used on any school- or library-owned computers?

Yes, school- or library-owned computers will use the supported access, services, connections, or network equipment.

YES

School-or library-owned computers must be CIPA compliant.

No, only third-party-owned computers will use the supported access, services, connections, or network equipment.

NO

NO

CIPA compliance is not required for school- or library-owned computers.

What Does CIPA Require?

3 Requirements of CIPA:

1) **Internet Safety Policy**
    - Libraries are required to adopt and enforce an Internet Safety Policy (ISP) that contains the 5 required elements
    - ISP is different than an Acceptable Use Policy (AUP)
        - AUPs are typically posted and/or signed by patrons/staff
    - ISP can be a high-level policy which is different than evolving day-to-day staff procedures
2) **Technology Protection Measure (Filter)**
3) **Public Notice and Hearing or Meeting**

Internet Safety Policy

Must address all of the following 5 elements:

- Access by minors to inappropriate matter on the Internet and World Wide Web;
  - *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*
- 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'.
  - *HTM 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."*

  - Minors = under the age of 17

Filter (Technology Protection Measure)

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

- The library must enforce the operation of the filter during the use of **its** computers with Internet access
  - Only library-owned computers must be filtered
  - Includes both at the library and when taken off-site
  - Applies to all library-owned computers, including computers not used by the public
  - Patron-owned computers, even if using library internet, are *not* required to be filtered
- The federal government has published no lists of sites that must be restricted nor has it set standards for blocking
- Text and e-mails are not specifically required to be filtered
- In addition to the content that must be blocked, libraries may block any content deemed inappropriate by local standards for minors
- Filtering can be done centrally by an Internet provider or at the server level on the library's LAN or WAN, or the filter can be individually installed on each computer (or combination of these)

Disabling a Filter

- An administrator, supervisor, or other person authorized by the library administration may disable the filter during use by an adult to enable access for bona fide research or other lawful purpose
- 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
- Filters can be set to different age-group levels
  - Example: very strict for young children, less restrictive for teens, least restrictive for adults
- Cannot be disabled for minors, ever
  - But if a filter catches legitimate content that is not harmful to minors (overblocked), they can request that staff unblock the site
- Cannot be permanently disabled

What if a Filter Fails?

- The FCC presumes that Congress did not intend to penalize libraries that act in good faith and in a reasonable manner to implement TPMs
- No TPM is 100% effective in preventing all such access. In its CIPA regulations, the FCC declined to adopt any type of standard on how effective a TPM must be
- A library must have policies and procedures to address any complaints in an expeditious manner. If a patron claims that too many allegedly illegal images are getting through the TPM, CIPA does not provide a venue for patrons to take legal action against the library
- Rather, we presume patrons can file a complaint with the FCC which will then initiate an investigation
  - The FCC can require a library to reimburse its E-rate discounts for any time it is out of compliance, but the Commission assumes that it “will rarely, if ever,” be called upon to take such action
  - The Institute of Museum and Library Services (IMLS) can withhold future payments to the library but it cannot retroactively recoup funds for any time a library is out of compliance

Public Notice and Hearing/Meeting

- The entity with responsibility for administration of the library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed Internet Safety Policy and technology protection measure (filter)
  - Hearing should have been held since August 2004
  - Advertise the meeting via email, flyers, phone call, or any way you deem appropriate for your library
- Additional meetings are not required – even if the policy is amended – unless those meetings are required by state or local rules or the policy itself
  - However, it is a good idea to periodically review your policy to ensure it has remained current

Acceptable Use Policies (AUP)

- AUPs are different than Internet Safety Policies
- AUPs typically stipulate constraints and practices that a user must agree to in order to access a computer or the Internet
- AUPs are not required by E-rate, but libraries are required to distribute AUPs (sometimes called Eligible Use Policies) to patrons who use the ECF-funded computers and/or hotspots
    - Note: USAC is requesting copies of random libraries' AUPs during the Form 472 BEAR invoicing process
- In addition, libraries are required to obtain a signed Statement of Unmet Need from each library patron prior to checking out ECF-funded computers and/or hotspots to patrons
    - Sample Unmet Needs Certification is available at: http://e-ratepa.org/wp-content/uploads/2021/08/Unmet-Needs-Library-Patron-Certification.docx
- AUPs and Unmet Needs Certifications may be signed electronically as part of the check-out process
- Both must be kept for 10-years

How is CIPA Compliance Certified?

- Libraries are required to certify annually their CIPA compliance on the E-rate Form 486
  - Options:
    - CIPA compliant
    - Not required to be CIPA compliant (rare)
    - 1st year in E-rate and are undertaking actions to become CIPA compliant (very rare)
  - If you requested ECF funding, and you already certified CIPA compliance on the Form 486 for FY 2021, no further certification was needed
- Entities filing E-rate consortia Form 471s are required to collect a signed Form 479 from each consortium member every year
  - Form 479 asks consortia member to certify CIPA compliance
  - After all 479s have been collected, then consortia lead can file the Form 486 to certify that all of their consortia members are CIPA compliant
  - Form 479 is a PDF form and signed forms should not be submitted to USAC unless specifically requested
- For ARP-IMLS funds used for internet services or connected devices, complete and submit this form with your application: https://www.statelibrary.pa.gov/Documents/For%20Libraries/Subsidies%20and%20Grants/LSTA/ContratorforaGrant/Internet%20Safety%20Certification%20form.pdf

What if You're Not CIPA Compliant?

- Every USAC audit requires the library to prove CIPA compliance for all recipients of service on the Form 471 application
- If deficiencies are found, 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
- Specific examples that have been addressed by the FCC:
  - If a library has complied in practice with its CIPA certification, but inadvertently left out one of the requirements in its written internet safety policy, the library could correct its policy as it was substantially compliant with the CIPA requirements.
  - If a 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.

How to Prepare for CIPA Audit

USAC AUDIT CHECKLIST

- ❑ Copy of the internet safety policy
- ❑ Documentation of the adoption of the internet safety policy
- ❑ A copy of the minutes and the date of the public hearing regarding the internet safety policy
- ❑ Documentation supporting that reasonable public notice was given for the public hearing
- ❑ A description of the Technology Protection Measure (filter) used
- ❑ A copy of a report (if applicable) or other documentation on the use of the filter for the funding year(s) subject to audit (i.e., reports from the service provider of internet sites blocked, bills from the service provider verifying that the filter was operational, etc.)
- ❑ Copy of filtering invoice/receipt (if applicable)
- ❑ Copies of:
  - FCC Forms 479, (Certification by Administrative Authority to Billed Entity of Compliance with the Children's Internet Protection Act (CIPA) Form), as applicable and/or
  - FCC Forms 486, (Receipt of Service Confirmation and Children’s Internet Protection Act Certification Form)

Your Questions…

Q1) Is the cost of filtering E-rate eligible?

A: No.

Q2) What can a library do if they have claimed to be CIPA compliant, but then realize they have fallen out of compliance?

A: Begin the process to get into full compliance right away.

Q3) Can you give recommendations on the best options for providing CIPA compliance? Server options as opposed to individual workstation options?

A: The Commonwealth cannot make recommendations for the best filtering software or appliance. Asking your colleagues is a good way to learn what others use in Pennsylvania.

Q4) Are there any rules about how recently a library has to have reviewed their Internet Safety Policy?

A: There is no E-rate rule related to how often you must review your Internet Safety Policy. However, it is a good practice for library directors to review all policies with the board of trustees on a regular basis. For a technology related policy that may change as technologies change, setting a reminder to review your technology related policies every two or three years, but no longer than five, might serve as a base level idea to start.

Your Questions…

Q5) Is it enough that we require parent signature by minor to use the internet?

A: Parental signature is not a CIPA requirement for minors to use the Internet. Parental permission may be written into your library’s Acceptable Use Policy or be part of the procedure you use to implement the policy, but on its own, that isn't enough for CIPA compliance. Refer to the full requirements.

Q6) Are there any free filters/products my library can use?

A: It is possible that there are free products, but we are not authorized to recommend any specific providers.

Your Questions…

Q7) Are systems required to have a CIPA policy even though they do not provide computers for public access?

A: In E-rate terms, a library system means a library with one or more branches. In this context, administrative offices of library systems are required to be CIPA compliant, even if their computers are not being used by the public.

If a “system” by PA terminology is applying for E-rate funding as a consortia lead only, they would not be required to be CIPA compliant if the consortia lead is not receiving E-rate eligible services (this would be rare).

However, a library must comply with CIPA if your library uses federal money to purchase one or more computers that will access the Internet, or uses federal money to purchase Internet access itself.

***

Your Webinar Questions…

Q8) If you check out hotspots to patrons, do they have to be filtered?

A: Hotspots are not required to be filtered under ECF; only all computers/laptops. If you are using IMLS funds to purchase hotspots with internet connectivity, you must certify CIPA compliance.

Q9) Can the public hearing be held during a regular board meeting or must be a separate hearing?

A: It can be held during a regular board meeting, as long as public notice has been given that you will be considering your Internet Safety Policy at the meeting.

Q10) If an adult patron asks for the filter to be disabled or for a particular page be unblocked, must the filter be disabled immediately (if deemed appropriate)?

A: The E-rate rules are silent on this issue. Your local procedures should prescribe the process for such requests, and who may disable the filter.

Your Webinar Questions…

Q11) Are circulating chrome books required to be filtered? What if they are only circulated to adults?

A: Yes, even if they are only loaned to adults. To be CIPA compliant, all library owned or leased computers, even those not purchased with federal funds, must be filtered.

Q12) What if we are missing signed Forms 479 for prior funding years?

A: You should obtain the signed forms right away – one for each missing year.

Q13) If you loan a kit with a laptop and a hotspot, you would have to filter, but if you just loan the hotspot you don't?

A: If you are covered by CIPA (highly likely), then all library-owned computers must be filtered, regardless of where they're used. Hotspots are not required to be filtered, as they are not defined as "computers."

Your Webinar Questions…

Q14) Is our library covered by our district library's Internet Safety Policy (they apply for E-rate on our behalf) or do we need our own?

A: If your library is its own administrative authority with its own budget, then you would need your own policy.

Q15) If you don't use E-rate or ECF funding for the hotspot/laptop loans, do they have to CIPA compliant, but you accept E Rate funding for your library Internet access?

A: If you accept E-rate, ECF or IMLS funding to purchase connected devices, then you are required to be CIPA compliant and must filter all library-owned computers, regardless of where those computers are used.

Q16) Does the source of funding for the Chromebooks affect whether they need filtering?

A: No, the source of funding for the Chromebooks is not a factor in determining whether you must filter. If you are CIPA compliant, all computers owned or leased by the library must have a filter.

Your Webinar Questions…

Q17) When do the USAC audits usually take place; are we given notice?

A: Audits are announced year-round. Notice is provided to applicants via e-mail with a follow-up call, and applicants are asked to provide the required documentation in about 14 days. Extensions are granted upon request.

Resources

- https://www.usac.org/e-rate/applicant-process/starting-services/cipa/
- https://www.fcc.gov/consumers/guides/childrens-internet-protection-act
- https://www.ala.org/ala/washoff/WOissues/civilliberties/cipaweb/cipa.htm
- https://www.ala.org/ala/washoff/WOissues/civilliberties/cipaweb/adviceresources/adviceresources.htm
- https://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/telecom/broadband/CIPA%20Compliance%20Scenarios%20in%20ECF_final_6.8.21.pdf
- Act of Nov 30, 2004, P.L. 1556, No. 197 Cl. 35