CIPA Compliance Hillstone Security Solutions

This paper discusses the legal requirements of the Children’s Internet Protection Act (CIPA) and how Hillstone’s robust security solutions can help schools and libraries demonstrate that they offer a safe and secure environment for minors.

Summary

The Children's Internet Protection Act (CIPA) federal law was enacted in 2000 to keep young users safe online. The law addresses concern about minors’ access to obscene, explicit or harmful content or pornography on Internet-connected devices in libraries and schools. CIPA requires libraries and K-12 schools to implement Internet filters and other “technology protection measures” to safeguard minors from harmful online content as a condition for the receipt of certain federal funding, such as E-rate funds.

Schools and libraries must be able to certify that they have an Internet safety policy and technology protection measures in place to filter Internet access to pictures that are: a) obscene, b) child pornography, or c) harmful to minors.

CIPA Requirements

Schools and libraries subject to CIPA are required to adopt and implement a policy addressing:

1. Access by minors to inappropriate matter on the Internet,
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications,
3. Unauthorized access, including “hacking” and other unlawful activities by minors online,
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors, and
5. Restricting minors’ access to materials that are harmful to them.

The Hillstone security services portfolio helps schools and libraries provide a filtered and protected environment for minors to safely access Internet content.

Hillstone Security Services to Address CIPA

The Hillstone security services portfolio includes:

- **StoneShield**: A rich set of firewall features that provide abilities such as monitoring and inspecting traffic, making rules-based policy decisions to allow or block specific traffic flows, and recognizing and filtering based on application characteristics. Sophisticated features including Abnormal Behavior Detection and Advanced Malware Detection provide additional protection against more subtle, newer or unknown threats by continuously monitoring and analyzing network behavior, detecting and protecting against anomalous behavior.

- **URL Filtering**: Dynamic web filtering with real-time categorization and database update to identify and restrict malicious or inappropriate web content or URLs.
- **Anti-Spam**: Real-time spam classification and prevention regardless of language, format or content to prevent network users from receiving inappropriate or unwanted communications.
- **IP Reputation**: Identify and filter traffic from risky IP addresses or source locations.
- **Anti-virus**: Virus and malware detection and prevention.
- **Intrusion Prevention**: Network intrusion detection and prevention.
- **Sandbox**: Detection and prevention of new and unknown malware.
- **Botnet C&C Prevention**: Discover intranet botnet and malicious C&C (command and control) connections.

CIPA Requirement	Hillstone Services and Features
1. Access by minors to inappropriate matter on the Internet.	• Application filtering: Each application can be filtered based on a description, risk factors, dependencies, and typical ports used. • Flow-based web filtering inspection. • Manually defined web filtering based on URL, web content or MIME header. • Comprehensive DNS firewall policy, restricting accessible Internet destinations. • Different web filtering profiles can be assigned to a user, group, or IP address. • IP reputation: Logging, dropping packets, or blocking traffic for different types of risky IP locations. • Firewall security policy based on application, role and geo-location. • Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols. • Filter files transmitted by HTTPS using SSL Proxy. • Additional web filtering features include Filter Java Applet, ActiveX or cookie; Block HTTP Post; Log search keywords.
2. Protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.	• Manually defined web filtering based on URL, web content and MIME header to block inappropriate direct communications sites and chat rooms. • IM identification and network behavior audit. • Real-time message classification and prevention regardless of the language, format, or content of the message. • 4 million anti-virus signatures to prevent inappropriate or insecure content or attachments from reaching users. • Virus scanning of compressed files. • Behavior-based advanced malware detection of more than 2000 known and unknown malware families including viruses, worms, trojans, overflow etc.

	• Support for SMTP and POP3 email protocols, with inbound and outbound detection.
3. Unauthorized access, including “hacking” and other unlawful activities by minors online.	• IP and domain whitelists. • User and device-based authentication. • User and device-based firewall and traffic filtering policies. • Using rich monitoring and reporting capabilities, bringing multiple sources of information together, the Hillstone system provides extensive network visibility and can identify contextual information to make proper blocking decisions. • Discover intranet botnet hosts by monitoring C&C connections.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.	• Firewall features to restrict or block access from outside the network. • User login and authentication for devices on the network. • Intrusion protection (IPS) with 8,000+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual or automatic push or pull signature updates, and an integrated threat encyclopedia. • Abnormal Behavior Detection models based on L3-L7 baseline traffic to reveal anomalous network and traffic behavior. • Hillstone devices support numerous local (on the device) and remote (SNMP) logging facilities for auditing, tracking and forensic purposes. • Network segmentation and definition of zones to protect and restrict access to certain parts of the network. By default, Hillstone devices deny all traffic between security zones or segments.
5. Restricting minors’ access to materials that are harmful to them.	• Firewall features optimized for content analysis of Layer 7 applications, providing granular control of web applications regardless of port, protocol, or evasive action. • Granular control over users, and user-groups, and what content they can access. • Security policies to restrict or block unauthorized applications. • Application, URL, and threat events statistics and monitoring. • Application Level Gateways and session support for detection and protection.