
2025
WISPAMERICA™
BROADBAND WITHOUT BOUNDARIES

Important Developments In Cybersecurity Rules And Policies At Federal Agencies

March 27, 2025 at 8:30 AM

Before We Get Started…

- Please mute your devices.

- Disclaimer:
  - The information contained in this presentation is general and is not offered as legal or other professional advice or direction.
  - This presentation is not intended to create an attorney-client relationship.
  - You are strongly encouraged to consult with your attorney(s), consultant(s), or financial advisor(s) if you have specific questions.
  - Any reliance on the information in this presentation is taken at your own risk.

Moderator & Speakers

Louis Peraertz, WISPA, VP of Policy lperaertz@wispa.org

Anand Chari, CEO, Kognitive Networks Anand.Chari@kognitive.net

Henry Ortiz, Borderhawk - henry.ortiz@borderhawk.com

Jeff Carlisle, Lerman Senter PLLC, - JCarlisle@lermansenter.com

Henry Ortiz, Esq.

- Cybersecurity & Privacy Compliance Advisor
- Framework based Cybersecurity compliance programs
  - HIPPA - Healthcare
  - CMMC – Dept. of Defense Contractors
  - NIST CSF - Telecommunications
- DBA / Secured IP / HFC
- Henry.Ortiz@BorderHawk.com
- https://www.linkedin.com/in/hjortiz/

Jeff Carlisle, Esq.

- Member, Lerman Senter
- Former Chief, FCC's Wireline Competition Bureau
- 25+ years experience in telecom and national security issues
- jcarlisle@lermansenter.com
- https://www.linkedin.com/in/jeffrey-carlisle-5379593/

Anand Chari

CEO and Co-founder, Kognitive Networks
30+ years experience in wireless telecom
Former CTO, Gogo, inflight wifi provider
Anand.chari@kognitive.net
https://www.linkedin.com/in/anand-chari/

Louis Peraertz

WISPA Vice President of Policy

Advisor to former FCC Commissioner Mignon Clyburn

More than 30 years of federal legal and regulatory advocacy experience

lperaertz@wispa.org

2025 WISPAMERICA
BROADBAND WITHOUT BOUNDARIES

Current Cybersecurity Related Reporting Rules

- Customer Proprietary Network Information (CPNI) certification.
  - Annual certification requirement on March 1.
  - Applies to Common carriers/ETCs and Interconnected VoIP providers.
  - Information that qualifies as CPNI.
    - Phone numbers called by a consumer
    - Frequency, duration, and timing of calls
    - Broadband data consumption
    - Web browsing and app usage history

Current Cybersecurity Related Reporting Rules

- Robocall Mitigation Database Certification.
  - Annual certification requirement on March 1 to verify accuracy of information submitted in database.
  - Applies to voice providers, intermediate providers, and gateway providers.

Current Cybersecurity Related Reporting Rules

- Supply Chain Report.
  - Annual certification requirement on March 31.
  - certify whether the provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service on the list of covered communications equipment and services.
  - Applies to broadband service providers.

CALEA & NPRM

Henry Ortiz, Esq. Jeff Carlisle, Esq.

CALEA & NPRM

- Important sequence of events:
  - **02/2024 CISA, NSA, FBI, other U.S. federal agencies**
    - Warn that “People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.
  - **2024 Q3/Q4 Salt Typhoon**
    - Infiltrated multiple U.S. telecommunications carriers, potentially accessing communications of senior U.S. political figures and collecting data on Americans.
    - CALEA Servers ➔ Communications Assistance for Law Enforcement Act
  - **Dec-4-2024 CISA Publication “Cybersecurity and Infrastructure Security Agency”**
    - "Enhanced Visibility and Hardening Guidance for Communications Infrastructure" ==> recommendations
    - “the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the communications sector to support its operations and associated day-to-day communication needs for corporate and organizational networks and services
  - **Media & Public / ==> FCC? / CISA? / Congress?**
    - Where are the regulations?
  - **01/02/2025 6th Circuit Decided Net Neutrality**
    - Limited the FCC's power to regulate Broadband service providers based on the “telecommunications service” provision of the Communications Act.

CALEA & NPRM

- **12/10/2024 Bill Introduced**
  - ==> Secure American Communications Act (Senator Wyden, Oregon, D)
    - Based on the Communications Assistance for Law Enforcement Act
    - Not based on “telecommunications service” provision of the Communications Act.
      - Telecommunications carriers must protect their networks
      - Mandatory ==> Independent 3rd party annual audits
      - Annual Reports. Signed by CEO, CIO, or equivalent, attesting compliance with the rules prescribed

- **01/15/2025**
  - FCC Declaratory Ruling:
    - Adopted: 01/16/2025
    - Section 105 of Communications Assistance for Law Enforcement Act (“CALEA”) affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications.
    - “we conclude that Congress has authorized the [FCC] to adopt rules that require telecommunications carriers to take specific steps to secure their networks”
    - A Covered Provider’s equipment, architecture, networks and network elements, and any element of a Covered Provider’s business that contributes to the provision of a service to the Covered Provider’s subscribers or customers and affects how a Covered Provider’s subscribers or customers receive that service.
    - CALEA extends not only to the equipment they choose to use in their networks, but also to how they manage their networks

NPRM

“Covered Providers”:

1. Facilities-based fixed and mobile broadband Internet access BIAS service providers
2. All broadcasting stations—including AM broadcast stations, FM broadcast stations (including low power FM broadcast stations and program originating FM booster stations), digital audio broadcasters,
3. All television stations—including low power television stations, television broadcast translator stations, and all analog television and digital television service providers; all cable systems (including digital cable systems and wireless cable systems); wireline video systems; wireline communications
4. Commercial radio operators; interconnected VoIP providers (including providers of outbound-only VoIP); telecommunications relay service (TRS) providers; satellite communications providers (including all space and earth station licensees, mobile satellite service providers, Direct Broadcast Satellite (DBS) providers, SDARS providers, geostationary orbit (GSO) and GSO-like satellite operations, non-geostationary orbit (NGSO) and NGSO-like satellite operations, Fixed Satellite Services,Earth Exploration-Satellite Services, satellite operators, and any other satellite communications provider that use space stations as a means of providing the public with communications);
5. Commercial mobile radio providers; wireless resellers and Mobile Virtual Network Operators (MVNOs); covered 911 service providers; covered 988 service providers; and international section 214 authorization holders. We hereinafter refer to these entities collectively as “Covered Providers”.

NPRM

- CALEA: Adopted Jan-2025
  - affirmatively requires telecommunications carriers to secure their networks from unlawful access

- **REQUIRED:**
- Audits: 3rd party (Audit teams)
- Create, update, and implement cybersecurity and supply chain risk management plans
- (NIST) Cybersecurity Framework (CSF)
- Covered Provider's CEO, Chief Financial Officer (CFO), Chief Technology Officer (CTO), or a similarly situated senior officer responsible for governance of the organization's security practices would be required to sign a Covered Provider's cybersecurity and supply chain risk management plans
- Comply within 12 months of publication
- Annually thereafter

Summary

- CALEA: Adopted Jan-2025
  - affirmatively requires telecommunications carriers to secure their networks from unlawful access
- NPRM:
  - Finalized by FCC (Audits, Risk Management Plans, Signed by C-Level executive, Annual)
    - Not yet published in the Federal Register (Request for comments)
    - January 20th Regulatory Freeze pending Review President Trump.
- Trend: Increased number of lawsuits from end-users
  - Negligence based.
    - *"What would a reasonable network operator do to protect the network and the subscribers against cyber attacks?"*
  - Contractual obligations, waivers of liability,
- Possible Implied obligations?
  - HIPAA CMMC

Ban Of Kapersky AntiVirus Software

Louis Peraertz

Ban Of Kapersky AntiVirus Software

- In 2021, the Justice Department asked the Commerce Department to investigate Kapersky because Russian laws compel companies, subject to Russian jurisdiction, to cooperate with Russian intelligence and law enforcement efforts.

- In June 2024, the Commerce Department published a Final Determination. “Kaspersky’s provision of cybersecurity and anti-virus software to U.S. persons, including through third-party entities that integrate Kaspersky cybersecurity or antivirus software into commercial hardware or software, poses undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons.”

- Any resale, integration, or licensing of Kapersky cybersecurity and antivirus software for purposes of resale or integration into other equipment is prohibited after 12 AM on September 29, 2024.

- https://www.federalregister.gov/documents/2024/06/24/2024-13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc

Ban Of Kapersky AntiVirus Software

- In July 2024, the FCC added Kapersky anti-virus software to the list of communications equipment and services that have been determined to pose an unacceptable risk to the national security of the United States. https://www.fcc.gov/supplychain/coveredlist

- In September 2024, the FCC issued a Public Notice announcing that any equipment that integrates cybersecurity or anti-virus software produced or provided by Kaspersky, or any of its successors or assignees, is prohibited from obtaining an equipment authorization from the FCC. https://docs.fcc.gov/public/attachments/DA-24-886A1.pdf

- CISA urges companies to review the FCC's covered list of equipment and services when developing your cybersecurity risk management plans. https://www.cisa.gov/news-events/alerts/2023/05/01/cisa-urges-organizations-incorporate-fcc-covered-list-risk-management-plans

Executive Order 14028

Louis Peraertz

How Biden’s EO 14028 Impacts Commercial Businesses

- Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," issued by President Biden on May 12, 2021, aims to strengthen US cybersecurity by modernizing federal systems, enhancing software supply chain security, establishing a cybersecurity review board, and improving incident response.
- Key Provisions
    - **Modernizing Federal Cybersecurity**:
        - The EO requires agencies to modernize their cybersecurity systems, adopt zero-trust architecture, and implement multi-factor authentication and encryption.
    - **Enhancing Software Supply Chain Security**:
        - The order emphasizes the importance of securing the software supply chain, requiring agencies to ensure that software they purchase from providers is secure.
    - **Establishing a Cybersecurity Safety Review Board**:
        - The EO creates a board to review and assess cybersecurity incidents and make recommendations for improvement. Board consists of federal and commercial experts.

How Biden’s EO 14028 Impacts Commercial Businesses

- Key Provisions
  - **Improving Incident Detection and Response:**
    - The order aims to improve the federal government's ability to detect, assess, and remediate cyber incidents by setting new reporting requirements and removing obstacles to public-private threat information sharing.
  - **Standardizing Federal Response Protocols:**
    - The EO aims to create a unified and effective federal response to cyber incidents.
  - **Strengthening the Cybersecurity Workforce:**
    - The EO recognizes the need for a skilled cybersecurity workforce and encourages investment in cybersecurity education and training.

How Biden's EO 14028 Impacts Commercial Businesses

- Key Provisions
  - **Focus on Critical Infrastructure**
    - The order emphasizes the importance of protecting critical infrastructure sectors, including energy, water, and healthcare, from cyberattacks.
  - **The Importance of Zero-Trust Architecture**
    - The executive order explains the importance for encouraging widespread use of a zero-trust cybersecurity principle to be adopted.
    - Mandates that federal agencies implement zero-trust principles.
  - **Cybersecurity Labeling for Consumers**
    - The order directs NIST to initiate two labeling programs on cybersecurity capabilities of Internet-of-Things (IoT) consumer devices and software development practices.

FCC NPRM On Border Gateway Protocol Risk Mitigation

Anand Chari. Jeff Carlisle, Esq.

FCC NPRM – voted June 6, 2024

- Border Gateway protocol (BGP) is a global inter-domain routing protocol used to route traffic across the Internet.
- BGP is, however, vulnerable to malicious actors falsifying routing information in order to redirect Internet traffic.
- In its Notice, the FCC asserted the authority under Titles II and III and Section 706 of the Telecom Act and CALEA to require broadband Internet access service (BIAS) providers to file BPG Routing Security Risk Management Plans.
- Adopted after Title II Order but before 6th Circuit reversal

Risk Management Plans

- Initially intended for only the 9 largest BIAS providers, but could extend to all; would require initial filing, annual updates, and specific data every quarter to measure implementation progress
- Would require BIAS providers to describe and attest to efforts they have made to create and maintain Route Origin Authorizations (ROAs) within the Resource Public Key Infrastructure
- Also require them to attest whether they have implemented Route Origin Validation at interconnection points
- Updates must be filed until ROAs cover at least 90% of a provider's IP address prefixes

Issues

- FCC criticized by Internet-related bodies as reacting to an ostensibly dire security issue by imposing reporting requirements rather than analyzing the practices and incentives that influence ROA implementation.
- WISPA and other industry groups directly questioned the FCC's authority to adopt any such regulations.
  - Even if Title II regulation had stood, BGP routing would not be considered a Title II telecommunications service.
  - Reversal of FCC's Title II Order eliminates major part of FCC's asserted authority.
- Chairman Carr is focused on national security (e.g., formed Council on National Security) but this proceeding may not be a high priority and he may be more willing to let multi-stakeholder processes lead.

FCC Cybersecurity Pilot Program for Schools and Libraries.

Anand Chari. Jeff Carlisle, Esq.

Introduction to the FCC's Cybersecurity Pilot Program

- The FCC Cybersecurity Pilot Program is a $200 million initiative aimed at enhancing cybersecurity for K-12 schools and libraries. (2024-2027)
- Funded/administered through USF, which also supports the E-Rate program.
- Designed to protect student data and critical infrastructure from rising cyber threats.
- Primary goal: Assess feasibility of long-term cybersecurity funding under E-Rate or a new program.

Eligibility Criteria

- Open to schools, libraries, and consortia that meet E-Rate program eligibility.
- Institutions do not need to be current E-Rate recipients to qualify.
- Selection criteria prioritized broad representation: large and small institutions, urban and rural, and Tribal entities.
- Applicants had to demonstrate cybersecurity needs and readiness to implement solutions.

Selection of Participants

- A total of 707 participants were selected: 645 schools and 62 libraries.
- Representation across all 50 states, with a focus on equitable distribution.
- Inclusion of Tribal institutions and rural schools to address cybersecurity disparities.
- Highly competitive selection process due to limited funding availability.

Eligible Services and Equipment

The FCC pilot funds various cybersecurity solutions, including:

- Next-generation firewalls (NGFWs) with intrusion prevention and deep packet inspection.
- Zero Trust Architecture (ZTA) to enhance access controls.
- Identity and access management (IAM) tools, including multi-factor authentication (MFA).
- Endpoint Detection and Response (EDR) for proactive cyber threat monitoring.
- Cloud security solutions to protect remote learning environments.
- Security information and event management (SIEM) for real-time monitoring.
- Network segmentation tools to prevent unauthorized access.

Application Process and Timeline

Two-part application process:

- Part 1 (Closed November 2024): Participants submitted applications demonstrating cybersecurity needs and implementation plans.
- Part 2 (Ongoing in 2025): Competitive bidding and vendor selection process.
- Participants must comply with federal procurement rules for cybersecurity services.
- Schools and libraries must report cybersecurity outcomes to help shape future funding.

Program Goals and Evaluation

Key goals of the program include:

- Assessing how cybersecurity services improve network protection in education.
- Collecting data on costs, effectiveness, and feasibility of cybersecurity funding.
- Helping policymakers decide on potential permanent funding under E-Rate or a separate long-term federal program.
- Informing future government cybersecurity funding initiatives for education and other sectors.

Opportunities for Service Providers

Why this matters for service providers:

- Schools and libraries need trusted cybersecurity partners to deploy solutions.
- Service providers with E-Rate expertise can expand into cybersecurity services.

Ways to support participants:

- Offer E-Rate consulting to help institutions maximize federal funding.
- Provide managed cybersecurity services aligned with pilot program goals.
- Educate schools and libraries on best practices for cybersecurity compliance.

Future Funding Opportunities

The FCC's cybersecurity pilot program is just the beginning—more government cybersecurity funding is expected, including:

- Potential E-Rate expansion to permanently fund cybersecurity solutions.
- Federal grants through the Cybersecurity & Infrastructure Security Agency (CISA).
- State-level funding for educational cybersecurity initiatives.
- Infrastructure Investment and Jobs Act (IIJA) and CHIPS Act—some funds allocated for cybersecurity infrastructure.

Opportunities for service providers & vendors:

- Stay informed on evolving federal cybersecurity initiatives.
- Align offerings with government procurement standards.
- Develop long-term cybersecurity solutions for educational institutions.
- Key takeaway: Service providers and vendors should position themselves early to support schools in navigating these funding opportunities.

Security Regulations & Compliance for K-12

Vendors can help your organization comply with a wide variety of regulations and mandates

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Protection of Pupil Rights Amendment (PPRA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Cybersecurity and Infrastructure Security Agency (CISA) Guidance
- Gramm-Leach-Bliley Act (GLBA) – Safeguards Rule
- State-Specific Laws
- Executive Order 14028 (Improving the Nation's Cybersecurity)
- K-12 Cybersecurity Act of 2021


2025 WISPAMERICA
BROADBAND WITHOUT BOUNDARIES

Additional Compliance Details

CIPA Compliance

Children's Internet Protection Act

CIPA requires schools and libraries receiving E-rate funding to create and enforce an **internet safety policy** that includes filtering harmful content, monitoring online activity, educating minors about cyber safety, and holding a public hearing to review the policy. Compliance also requires implementing technology to **block inappropriate content** and actively ensuring network security.

How vendors help organizations comply with CIPA

- ✓ **Content Filtering** - Block harmful and inappropriate content
- ✓ **Zero Trust Security (ZTNA) with Identity and Access Management (IAM)** – User resource use authentication
- ✓ **Historical Monitoring & Reporting** – Track network activity, generate audit logs for compliance documentation
- ✓ **Cloud-Based Centralized Management** – Single interface for updates and enforcement, across all campuses
- ✓ **Network Segmentation** – Separate user traffic and administrative networks for enhanced security

FERPA Compliance

Family Education Rights and Privacy Act

FERPA requires schools to protect the privacy of student education records, ensuring that student data is only accessed by authorized individuals and is safeguarded from unauthorized disclosure. Compliance includes implementing **secure access controls**, **encrypting sensitive data**, and maintaining **audit logs** to monitor access and data use.

How vendors help organizations comply with FERPA

- ✓ **Data Encryption –** Secure VPNs, point to point & point to hub
- ✓ **Access Controls –** Network policy for multi-tenancy
- ✓ **Monitoring – C**omprehensive logs and reports

COPPA Compliance

[Children's Online Privacy Protection Rule]

COPPA protects the online privacy of children under 13 by requiring schools and educational technology providers to obtain parental consent before collecting personal information from students. Compliance also requires **limiting data collection to what's necessary for educational purposes** and **providing parents with access to review or delete their child's information**.

How vendors help organizations comply with COPPA

- ✓ **Custom Content Filtering** – Limit access to educational sites and resources
- ✓ **Captive Portal** – Network access usage controls on a per user, per device level
- ✓ **Historical Usage Reports** – Logs of individual user activity, downloadable multi-format reports
- ✓ **Anonymity Controls** – Anonymize individual user data

K-12 Cyber Security Act of 2021

Cyber Security Act

The K-12 Cybersecurity Act of 2021 emphasizes the need for stronger protections in schools by requiring secure access controls, multi-factor authentication, and robust network security to safeguard student data. Compliance involves implementing regular cybersecurity training, **monitoring for threats**, **securing school devices and IoT systems**, **maintaining system updates**, and establishing a tested incident response strategy to defend against cyber risks.

How vendors help organizations comply with the Cyber Security Act

- ✓ **IPS Threat Monitoring** – Detect malicious activity and block threats using Cisco Talos ruleset
- ✓ **Built-in Firewall** – Intuitive rule creation with comprehensive logging
- ✓ **System Lifecycle Management & Updates** – Logs of individual user activity, downloadable multi-format reports

BEAD

Henry Ortiz, Esq.

2025 WISPAMERICA
BROADBAND WITHOUT BOUNDARIES

BEAD

- Regulations:
  - BEAD references EO 14028 and required attestations operational NIST cyber risk management plans and Supply Chain Management plans (BEAD applicants)
  - DOJ / Civil Cyber-Fraud Initiative / False Claims Act / 2023 $2.68 billion in settlements (whistleblowers)
  - State Broadband Offices (Allow to expand): 3rd party audits, mandatory incident response plans.
- Good:
  - BEAD funding to train staff on cyber risk management

Funding and Business Opportunities

Anand Chari. Jeff Carlisle, Esq.

HIPAA ePHI Security Rules

- Already providing professional services to healthcare providers?
  - MSP
  - MSSPs
  - Rural Hospitals
- NPRM ➔ ePHI Security Rules
  - 180 days to comply
  - Advisory / Consulting


THANK YOU