Broadcasting
Cable
Satellite
Wireless
Wireline

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Communications Sector Coordinating Council

ANNUAL REPORT 2024

Staying Ahead of the Threats

In the ever-evolving landscape of national security and emergency preparedness, the communications sector plays a pivotal role. As we delve into the accomplishments of last year and into 2024 it becomes evident that robust and resilient communications networks are essential for safeguarding our nation.

The communications sector faced broadly impactful security events that underscored the need to reexamine resiliency and national security and emergency preparedness (NS/EP). Cyber threats, both sophisticated and persistent, targeted critical infrastructure networks. These attacks ranged from ransomware incidents crippling critical enterprises to state-sponsored attacks that jeopardize availability of essential services.

The value of the communications sector's public-private partnership lies in its ability to strengthen resilience, share critical information, and forge innovative solutions—all vital components for safeguarding our nation during emergencies.

- In 2023, Google, Amazon, and Cloudfare faced the **largest DDOS attack in their company's history.**
- According to the annual McKinsey Global Survey with respondents from a broad range of industries, just **32% stated they were mitigating generative AI inaccuracies**, while **38% stated they mitigate cybersecurity risks.**
- The total cost of a data breach was at an **unparalleled 4.45 million in 2023**, having increased 15% in the past three years.
- In 2023, the U.S. saw **28 weather/climate disaster events with losses exceeding $1 billion each.** These events included a drought, four floods, 19 severe storms, two tropical cyclones, one wildfire, and one winter storm.

CSCC Priorities for Engagement with Government Partners

ALIGNMENT. Strategically aligned efforts are the foundation of successful efforts by bringing all stakeholders to the table and more effectively targeting resources. Streamlining participation in government initiatives has been a major focus.

TRANSPARENCY. CSCC members advocate for and model a culture of transparency to customers and government entities on how we handle security and resilience related issues.

COLLABORATION. CSCC members support enhancing and improving intelligence and information sharing to evolve into joint operational collaboration, including through voluntary partnerships.

INCLUSION. With CSCC support, small- and medium-sized business (SMB) members can participate robustly in programs, protections, and related initiatives, no matter their size and specialty.

About CSCC

Chartered in 2005, the communications sector coordinating council (CSCC) coordinates industry engagement with the U.S. Government on cyber and infrastructure security, resilience, and risk reduction.

> **“At CISA, partnership and collaboration are our foundation and the lifeblood of what we do. Information sharing and cooperative action—across both public and private sectors—is essential to our goal of raising the nation’s collective defense.”**
>
> **Jen Easterly | Director, Cybersecurity and Infrastructure Security Agency**

Scope of Partnership Engagement

CSCC addresses areas that are most vital to protect our nation’s critical infrastructure and to promote its resilience.

Emerging Technologies. In 2023, CSCC instituted the Emerging Technology Committee to analyze, assess, and address upcoming areas of risk for the Communications Sector through a series of impact reports. The first of these, titled The Engineer Who Cried Quantum, covered the upcoming transition to post-quantum cryptography. The report notes the many barriers to this transition, including dependence on the IT Sector, changes to protocol standards, and the underlying limitations of the proposed solutions themselves. It also outlines suggestions for the federal government that would help this transition from the creation of testbeds at the National Cybersecurity Center of Excellence to making it easier to engage in knowledge exchange with international partners.

Secure Internet Routing. CSCC members are global leaders in implementation of secure Internet routing tools and protocols and engaged with multiple federal agencies to explain their widespread deployment of Border Gateway Protocol (BGP) security tools and the need to promote such practices across the Internet ecosystem. In 2023, CSCC members shared their cutting-edge work with the FCC at the agency’s BGP Security Workshop.

National Cybersecurity Strategy. In 2023, the Administration released its National Cybersecurity Strategy (NCS) and Implementation Plan. CSCC members continue to share input with the Office of the National Cyber Director and are working to implement the NCS, while considering the allocation of industry resources needed to effectively protect critical infrastructure, and national and economic security.

NIST Cybersecurity Framework Version 2.0. Communications sector stakeholders continue to utilize and champion the NIST Cybersecurity Framework, which has succeeded in helping domestic and international organizations assess their cybersecurity risk for nearly a decade. CSCC members are providing input, including through written comments and workshop participation, as NIST targets early 2024 to finalize Version 2.0. The sector looks forward to working within an updated voluntary framework that is compatible with other government efforts and preserves the level of thoughtful and flexible guidance that stakeholders have come to rely on.

Cybersecurity in Subsidized Broadband Buildouts. Pursuant to NTIA's Broadband Equity, Access, and Deployment (BEAD) Program Notice of Funding Opportunity, and throughout the state allocation and planning process, CSCC members continue working to ensure that subsidized broadband networks include foundational cybersecurity and supply chain security best practices.

U.S. Cyber Trust Mark. The FCC proposed a voluntary cybersecurity labeling program intended to provide consumers with clear information about the security of IoT devices. Qualifying devices that meet established security standards would bear a U.S. Cyber Trust Mark—similar to the ENERGY STAR mark that helps consumers identify energy-efficient appliances. The program would also enable consumers to compare IoT devices and access the most up-to-date security information of each device.

NIST AI Risk Management Framework 1.0. NIST's AI RMF provides a much-needed set of guidance for organizations thinking about creating AI systems in a trustworthy and responsible manner. It is a voluntary framework that is adaptable to future changes in AI. Applicable across varying sectors and organizational sizes, the AI RMF details risk mitigations that can be used in the design, development, and deployment stages of the AI lifecycle.

NIST has also created a Generative AI Public Working Group (GAI-PWG) to build upon the work of the AI RMF. This working group consists of public and private sector members who will offer guidance on how the AI RMF can be used to support generative AI growth, aid NIST in their work on the generative AI lifecycle and risk management and identify ways generative AI can address sector specific challenges and needs.

President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023) required the Cybersecurity and Infrastructure Security Agency (CISA) to evaluate AI risk categories and risk mitigations. Although not required, CISA sought the help of CSCC. The CSCC helped them to distill their definition of high-risk AI categories and place more attention on AI use cases. This effort is emblematic of the productive partnership between CISA and the Communications sector.

The President's National Security Telecommunications Advisory Committee. CSCC member companies and individuals serve in many capacities on the

President's NSTAC including as members, subcommittee leads, and subcommittee members. In 2023, the NSTAC drafted *Letter to the President on Securing Next Generation Wireless Telecommunications and Report to the President on Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors;* published *Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem*, and was tasked with conducting a study on *Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*.

Enduring Security Framework. Through the ESF, CSCC members focused on developing architectural, design and management practices to ensure security of 5G network slices, including internetworking connectivity (i.e., multi-carrier beyond 5G). In 2023, ESF industry and government experts published its second of a two-part series on *5G Network Slicing, 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance*, which focuses on identified threats to network slicing and industry-recognized best practices. The ESF also produced stakeholder guidance, *Recommended Best Practices for Administrators - Identity and Access Management*.

DHS SCRM Task Force. The Department of Homeland Security (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force consists of government representatives, as well as stakeholders from the Communications and IT sectors. Initiated in 2018, the task force identifies obstacles and presents solutions to create a more robust supply chain. They have continued to advance efforts for Hardware Bills of Materials (HBOM), Small and Medium-sized Businesses (SMB), Software Assurance, and Product Marketing. This past year the task force released multiple tools and guides, such as HBOM's "Hardware Bill of Materials Framework for Supply Chain Risk Management" and SMB's "Securing SMB Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks" and "Empowering SMBs: A Resource Guide for Developing a Resilient Supply Chain Risk Management Plan."

Communications Information Sharing and Analysis Center. Throughout 2023, Comm-ISAC government and industry partners worked to deepen our long-standing public-private collaboration. As always, the ISAC worked closely with partners in response to incidents and periods of heightened risk, including the conflict between Israel and Hamas, the devastating fires in Maui, other natural disasters, and multiple special events.

In 2024, the ISAC plans to finalize additional standard operating procedures, stand up a national capital region working group, deepen member-to-member operational cybersecurity information sharing, identify potential communications sector support to election resilience, and enhance sector use of the Homeland Security Information Network as a tool for unclassified information sharing.

Throughout 2023, the ISAC also worked to facilitate long-term sector resilience activities. At the sector level, we finalized ISAC standard operating procedures to ensure effective multi-directional information sharing among government and industry partners, continued work to counter social engineering campaigns against the sector, and mitigated physical threats to communications cables and other infrastructure. Industry and government partners also collaborated to improve preparedness through a spring workshop, establish best practices for state and local planners in advance of the 2023 and 2024 eclipses, and re-establish routine sharing of classified information.

The Comm-ISAC engaged other critical infrastructure sectors through the cross-sector resiliency forum with energy partners, a tri-sector tabletop exercise with energy and finance, and through the National Council of ISACs (NCI) with other sectors, including participating in the "NCI Day on the Hill" with a congressional member and staff. Comm-ISAC members and leadership also "took the show on the road," traveling throughout the U.S. from California to Texas to Colorado—and even internationally, travelling to Turkey and hosting a delegation from the Japanese IT and Communications ISAC—to promote public-private activities that enable greater communications resilience.

Joint Cyber Defense Collaborative. CSCC members continue to partner in the JCDC by contributing to the collaborative action framework for coordinating partner actions, building and enforcing resilience, and establishing channels and processes. In 2023, the JCDC's operational collaboration was particularly effective in identifying and preventing ransomware intrusions and offering support to mitigate the effects of such attacks on victims and aid in their recovery.

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII. CSRIC makes recommendations to the FCC on the implementation of best practices to promote the security, reliability, and resiliency of communications systems, and wrapped up its eighth iteration in June 2023. As with all previous iterations, CSCC members offered substantive contributions to shape the Council's work and figured prominently in leadership and contributory roles in all six working groups, including developing reports—5G Signaling Protocols Security; Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment; Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks; 911 Services Over Wi-Fi; Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure; and Leveraging Mobile Device Applications Firmware to Enhance Wireless Emergency Alerts.

EXECUTIVE COMMITTEE

Officers & Liaisons

Robert Mayer, Chair (USTelecom - The Broadband Association)

Kathryn Condello, Vice Chair (Lumen) & NSTAC Liaison

Rudy Brioché, Secretary (Comcast) & IT-SCC Liaison

Chris Boyer, Treasurer (AT&T)

Paul Eisler, Chief of Staff (USTelecom - The Broadband Association)

Joe Viens (Charter) & Comms ISAC Liaison

Members

Jessica Almond (CableLabs)

Colin Andrews (Telecommunications Industry Association)

Jason Boswell (Ericsson)

John Hunter (T-Mobile)

John Marinho (CTIA)

Christopher Oatway (Verizon)

Jenny Prime (Cox)

Tamber Ray (NTCA – The Rural Broadband Association)

Loretta Polk (NCTA – The Internet & Television Association)

Larry Walke (National Association of Broadcasters)

STANDING COMMITTEES

Administrative Committee

Rudy Brioché, Chair (Comcast)

Finance Committee

Chris Boyer, Chair (AT&T)

WORKING COMMITTEES

Cybersecurity Committee

Focuses on cyber initiatives and developments; provides technical advice; supports related activities and provides input to the Executive Committee on appropriate policy considerations.

Robert Cantu, Co-Chair (NCTA – The Internet & Television Association)

Paul Eisler, Co-Chair (USTelecom - The Broadband Association)

Emerging Technologies

Focuses on the impact of the new and developing technologies, such as post-quantum cryptography, artificial intelligence, and machine learning on role, products, and services of the communications sector.

Vaibhav Garb, Co-Chair (Comcast)

Taylor Hartley, Co-Chair (Ericsson)

Justin Perkins, Co-Chair (CTIA)

Infrastructure and 5G Committee

Concentrates on initiatives and developments involving critical infrastructure for all segments of the communications sector with a specific focus on 5G.

Chris Boyer, Co-Chair (AT&T)

John Marinho, Co-Chair (CTIA)

Chris Oatway, Co-Chair (Verizon)

Operational Coordination Committee

Coordinates incident response, continuity of government, and information sharing initiatives with the Communications ISAC, ESF#2 (Communications), other ISACs, and government & industry partners.

Chris Anderson, Co-Chair (Lumen)

Joe Viens, Co-Chair (Charter)

Outreach, Plans, and Reports Committee

Executes the CSCC's outreach and education strategies using CSCC assets and capabilities to improve awareness of sector activities.

Elizabeth Chernow, Co-Chair (Comcast)

Stephanie Woods, Co-Chair (Lumen)

Small and Mid-size Business Committee

The SMB Committee focuses on issues relevant to small and mid-sized communications companies.

Tamber Ray, Co-Chair (NTCA – The Rural Broadband Association)

Larry Walke, Co-Chair (National Association of Broadcasters)

Supply Chain Committee

Focuses on security and risk management issues related to global supply chain of the communications sector.

Colin Andrews, Co-Chair (Telecommunications Industry Association)

Traci Biswese, Co-Chair (NCTA - The Internet & Television Association

Jessica Cohen, Co-Chair (Verizon)

ACKNOWLEDGEMENTS

The CSCC is grateful for its partnership with the Department of Homeland Security, which is its Sector Risk Management Agency.

The CSCC would also like to thank the federal government partners its members work closely with across a broad range of venues and workstreams.

For more information visit
www.comms-scc.org

CSCC MEMBER COMPANIES

- 3U Technologies
- ACA Connects
- Altafiber
- Association for International Broadcasting
- Alliance for Telecommunications Industry Solutions
- AT&T*
- Bandwidth
- CableLabs
- Charter
- Comcast*
- Competitive Carriers Association
- CompTIA
- Consolidated Communications
- Consumer Technology Association
- Cox*
- CTIA - The Wireless Association
- Cumulus Media
- Ericsson*
- Frontier
- General Dynamics Information Technology
- Hubbard Radio
- Hughes Network Systems
- iconectiv
- Internet Security Alliance
- Iridium*
- Juniper Networks
- Lumen*
- National Association of Broadcasters
- NCTA - The Internet & Television Association
- NEC Corporation of America
- Neustar
- NineStar Connect
- North American Broadcasters Association
- Nsight
- NTCA - The Rural Broadband Association
- Nippon Telegraph and Telephone America
- Pioneer Telephone Cooperative
- Samsung
- Satellite Industry Association
- Scripps
- Sinclair
- Telecommunications Industry Association
- Telephone and Data Systems, Inc.
- T-Mobile*
- U.S. Cellular
- USTelecom - The Broadband Association
- Utilities Technology Council
- Verizon*
- Windstream
- WNYC
- WTA – Advocates for Rural Broadband

**Denotes CSCC members on the President's National Security Telecommunications Advisory Committee (NSTAC).*

CONTACT:

Chair: Robert Mayer, USTelecom - The Broadband Association
rmayer@ustelecom.org

Vice Chair: Kathryn Condello, Lumen
kathryn.condello@lumen.com