COMMUNICATIONS SECTOR COORDINATING COUNCIL

COMMUNICATIONS SECTOR COORDINATING COUNCIL

ANNUAL REPORT 2025

ABOUT THE 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

Introduction

At a time when government and private networks are under constant attack, public-private partnership is more important than ever to foster information sharing, identify actionable insights, and collaboratively iterate to enhance the security and resiliency of our communications networks.

Sophisticated and persistent cyber threats target most, if not all, critical infrastructure sectors, particularly healthcare, information technology (IT), and energy. These attacks range from ransomware incidents crippling critical enterprises to state-sponsored attacks that jeopardize sensitive data and—in some instances—the availability of essential services.

- According to a 2024 KPMG[1] survey of C-Suite security leaders of large businesses from a mix of industries, **40% experienced a cyber-attack in the preceding year**, and **76% are concerned about the growing sophistication of new cyber threats**.
- The total cost of a data breach in 2024 reached[2] a historic high at **$4.88 million, a 10% increase** from the previous year.
- In 2024, the U.S. saw[3] **27 weather/climate disaster events** with losses exceeding **$1 billion each**. These events included a drought, a flood, 17 severe storms, five tropical cyclones, one wildfire, and two winter storms.

The Communications Sector Coordinating Council (CSCC)—in collaboration with partners across other sectors and government—helps critical infrastructure owners and operators prepare for, address, and recover from these disruptive events.

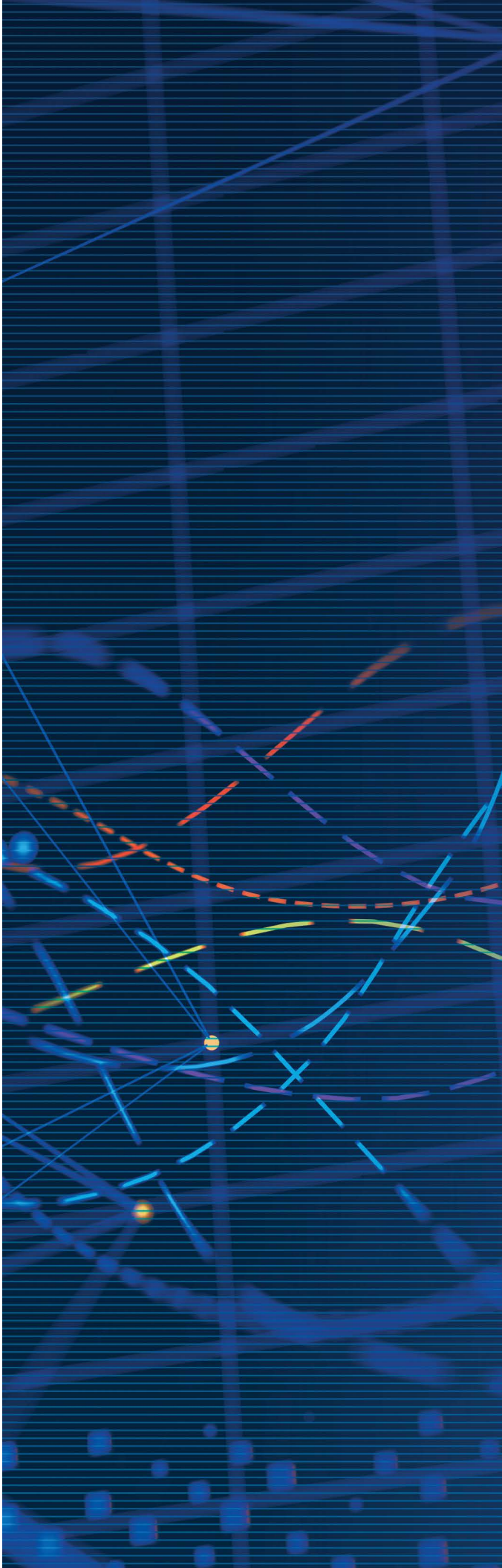
The communications sector itself faced broadly impactful security events in 2024 due to IT network and equipment vulnerabilities, and requiring significant response efforts that will inform critical investments in resiliency and national security and emergency preparedness in 2025 and beyond. For example, last year the Chinese state-sponsored advanced persistent threat, Salt Typhoon, attacked communications providers to steal sensitive U.S. data. American communications providers responded rapidly—in partnership with federal law enforcement and national security agencies, industry partners, and private cybersecurity firms—to investigate and address the incident as quickly as possible.

Investments made in operational partnerships over the last several decades are enabling the communications sector to work hand-in-hand with government counterparts to respond to, remediate, and recover from this espionage attack. Over the last year, key stakeholders collaborated through the President's National Security Telecommunications Advisory Committee (NSTAC[4]) and shared real-time intelligence and response efforts through the Cybersecurity and Infrastructure Security Agency (CISA) Joint Cyber Defense Collaborative (JCDC[5]). The Sector engaged with the White House Uniform

Coordination Group to help interagency efforts to assess and mitigate impacts and with CISA and the Federal Bureau of Investigation (FBI) to disseminate joint guidance[6] to industry on hardening networks in response to Salt Typhoon.

These forums—and the relationships fostered within them—provide a vital foundation for the work ahead. As Federal Communications Commission (FCC) Chairman Brendan Carr observed[7], addressing this attack requires "working closely with the intelligence community officials and the network providers that have been targeted..., conveying in real time the remedial steps that are necessary to restore the integrity of our networks—and ensuring that providers are implementing them," and "taking a series of actions that will restore America's deterrence and harden our networks going forward."

The communications sector is not alone in having faced significant attacks. From the Microsoft Exchange hack in early 2024 to the Citrix Bleed software vulnerability in 2023, recent events underscore the immense value of the communications sector's public-private partnerships and the foundations it relies on for rapid response. As the sector works to enhance network security in 2025, this partnership will be more vital than ever to ensuring our national security and emergency preparedness.



CSCC PRIORITIES For Engagement with Government Partners

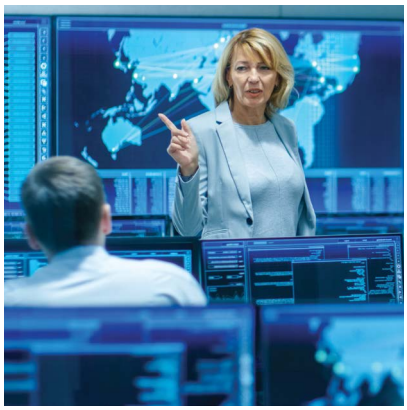
ALIGNMENT. Strategically aligned efforts are the foundation of successful efforts by bringing all stakeholders to the table and more effectively targeting resources. Streamlining participation in government initiatives has been a major focus.

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.

Scope of Partnership Engagement



CSCC ACCOMPLISHMENTS AND ACTIVITIES

Communications Information Sharing and Analysis Center. The Communications ISAC (Comm-ISAC) had a successful year in preparedness, capacity-building, response, and special event coordination. The ISAC's classified information-sharing programs continued to grow, bringing additional participants and perspectives into a robust information exchange, as it continued to work toward more robust and survivable coordination channels for response.

The Comm-ISAC participated in a range of exercises, including CyberStorm IX, a tri-sector continuity of the economy exercise, and the Critical Infrastructure Cybersecurity Tabletop Exercise.

In addition, the sector supported security and resilience coordination efforts for numerous special events including the national party conventions and election-day security coordination. These preparedness efforts were put to the test during response and restoration from Hurricanes Beryl, Helene, and Milton, as well as a nation-state attack targeting U.S. critical infrastructure.

Sector coordination with CISA also enables sector association members to inform and educate individual entities regarding cyber-related policy and technical developments. For example, the National Association of Broadcasters administers an industry committee in which members share expertise on systems and processes for reducing the risk of cyber disruptions, and offers venues at conventions and conferences for cyber experts to further educate broadcasters.

> **The Comm-ISAC, marking its 8th year of cooperation with the Japan ICT ISAC and Ministry of Internal Affairs and Communication, participated in successful international collaboration meetings in Tokyo and in the U.S. CISA representatives participated alongside industry in both meetings. Planning for additional collaboration is underway as the Comm-ISAC works to build on this effective partnership.**

Secure Internet Routing. The White House Office of the National Cyber Director (ONCD) in 2024 released a report[8] endorsing a risk-based, industry-led roadmap to secure internet routing. The report gratefully acknowledges the communications sector's "expertise, insight, contribution and inputs" in developing the roadmap. CSCC members have been touting their global leadership in implementation of secure internet routing tools and protocols and have engaged with multiple federal agencies to explain their widespread deployment of cutting-edge Border Gateway Protocol

(BGP) security tools and the need to promote such practices across the internet ecosystem. Building on the report's recommendations, CSCC members are leveraging their expertise as participants in a joint working group with CISA, ONCD, and IT sector stakeholders to lay the foundation for workstreams to advance the framework, as well as an implementation playbook.

Emerging Technologies. The CSCC's Emerging Technology Committee, now entering its second year, continues 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.

U.S. Cyber Trust Mark. In March 2024, the FCC adopted rules establishing a voluntary cybersecurity labeling program to provide consumers with clear information about the security of IoT products. Qualifying products that meet established security standards will bear a U.S. Cyber Trust Mark—similar to the ENERGY STAR mark that helps consumers identify energy-efficient appliances. The program will also enable consumers to compare IoT products and access relevant security information for each product.

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 2024, the NSTAC produced a Letter to the President on Dynamic Spectrum Sharing and a Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices. It also launched a workstream on baseline security principles for cloud service offerings.

Enduring Security Framework. Through the ESF—a collaboration of experts across the U.S. government, information technology, communications, and the defense industrial base sectors—CSCC members have 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 2024, ESF published recommendations for increasing U.S. participation and leadership in standards development. It also served as a forum for industry to develop a playbook on remediating and recovering from Volt Typhoon and Salt Typhoon.

Key Government Reports and Activities

National Cybersecurity Strategy. In May 2024, the Biden Administration released the second version of its National Cybersecurity Strategy (NCS) and Implementation Plan. CSCC members shared 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. Following robust engagement and input from CSCC members, in February 2024, NIST released Version 2.0 of its foundational Cybersecurity Framework. 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. As stakeholders update their cybersecurity and supply chain risk management practices to align to the updated framework, 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.

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.

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.

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

a Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle.

Joint Cyber Defense Collaborative. CSCC members continued 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.

CIRCIA Implementation. In 2024, CSCC members provided robust feedback to CISA on implementation of the Cyber Incident Reporting for Critical Infrastructure Act, including via a cross-sector letter recommending key revisions to CISA's proposed rules to support an effective program that produces actionable insights to enhance U.S. critical infrastructure security. CSCC association members also filed segment-specific comments on CISA's proposals, such as NAB comments that illuminated the link between CIRCIA and functionality of the Emergency Alert System.

Communications Security, Reliability, and Interoperability Council (CSRIC) IX. CSRIC makes recommendations to the FCC on the implementation of best practices to promote the security, reliability, and resiliency of communications systems and launched its ninth iteration in June 2024. As with all previous iterations, CSCC members are poised to offer substantive contributions to shape the Council's work, figuring prominently in leadership and contributory roles in all three working groups—Harnessing Artificial Intelligence/Machine Learning to Ensure the Security, Reliability, and Integrity of the Nation's Communications Networks; Ensuring Consumer Access to 911 on All Available Networks As Technology Evolves; Preparing for 6G Security and Reliability. Each working group is tasked with developing one or more reports between March 2025 and 2026.

ENDNOTES

1 https://kpmg.com/kpmg-us/content/dam/kpmg/corporate-communications/pdf/2024/2024-kpmg-cybersecurity-survey-findings.pdf

2 https://www.ibm.com/reports/data-breach

3 https://www.ncei.noaa.gov/access/billions/#:~:text=In%202024%2C%20there%20were%2027,and%202%20winter%20storm%20events

4 https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee

5 https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

6 https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

7 https://x.com/BrendanCarrFCC/status/1879674875973165368/photo/1

8 https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2024/sep/cs2024_0151a.pdf

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)

Shelley Blakeney (T-Mobile)

Taylor Hartley (Ericsson)

John Marinho (CTIA)

Christopher Oatway (Verizon)

Jenny Prime (Cox)

Tamber Ray (NTCA – The Rural Broadband Association)

Loretta Polk (NCTA – The Internet & Television Association)

Samuel Visner (Netcracker)

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.

Jayati Dev, 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 MEMBERS represent communications sector critical infrastructure owners/operators, their designated trade associations, and standard setting bodies, manufacturers, suppliers, and vendors of communications equipment, software, and services. The sub-sectors of the communications sector are broadcasting, cable, satellite, wireless, and wireline.

CSCC MEMBER COMPANIES

3U Technologies
ACA Connects
AltaFiber
Association for International Broadcasting
ATIS
AT&T*
Alliance for Telecommunications Industry Solutions
Bandwidth
CableLabs
Calix
Charter Communications
Comcast*
Competitive Carriers Association
CompTIA
Consolidated Communications
Consumer Technology Association
Cox Communications*
CTIA - The Wireless Association
Cumulus Media
Ericsson*
Frontier
General Dynamics Information Technology
Hubbard Radio
Hughes Network Systems
iconectiv
Internet Security Alliance
Iridium Communications*
Juniper Networks
Lumen Technologies*
National Association of Broadcasters
NCTA - The Internet & Television Association
NEC Corporation of America
Netcraker Technologies
Neustar
New York Public Radio
Nex-Tech
Nine Star Connect
Nippon Telegraph and Telephone America
Nokia
North American Broadcasters Association
Nsight
NTCA–The Rural Broadband Association
Oracle
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 Telecom Council
Verizon*
Windstream
WTA – Advocates for Rural Broadband

The asterisk (*) denotes members represented 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

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL