CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

COMMUNICATIONS SECTOR COORDINATING COUNCIL

ANNUAL REPORT 2026

CONNECTING THE FUTURE SECURING THE NATION

Message from the Chairs

We live in an era where connectivity is no longer just a utility; it is the central nervous system of our economy, our democracy, and our daily lives. From the seamless flow of financial data to the critical lifeline of a 911 call, the Communications Sector underpins every aspect of modern society.

This year, the Communications Sector Coordinating Council (CSCC) faced a threat landscape that was as dynamic as it was demanding. Yet, through every challenge—whether born of nature or malicious intent—our resolve remained unshaken. This Annual Report is not just a summary of activities; it is a testament to the power of partnership. It details how competitors became collaborators in the name of national security, and how the private sector and government worked in lockstep to forge a resilience that is the envy of the world.

As we look toward the horizon, we do so with a clear mission: to ensure that no matter the storm, the signal remains strong.

Robert Mayer, *Chair, CSCC*
SVP, Cybersecurity & Innovation, USTelecom

Kathryn Condello, *Vice-Chair, CSCC*
Lumen Fellow, NS/EP

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.

CSCC PRIORITIES

For Active Engagement with Government Partners and Key Stakeholders

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.

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

Public-Private Collaboration Leads to Results

Historically, the government has turned to private industry during times of crisis (e.g., WWII) to repurpose manufacturing and financial capabilities for national defense. Today, this reliance has evolved into a partnership model where private companies help secure digital infrastructure and critical services.

CSCC COMMITTEE FOCUS DURING 2025

EMERGING TECHNOLOGY: Collaboration with NIST on AI cybersecurity frameworks.

CYBERSECURITY: Threat evaluation reports, and enhanced intelligence sharing.

INFRASTRUCTURE AND 5G: Industry-led resilience testing through DHS exercises.

SUPPLY CHAIN: Addressing risks from foreign-linked technologies and advocating for clearer government procedures.

SMALL- AND MID-SIZED BUSINESSES (SMB): Tailored outreach and guidance for small- and mid-sized businesses.

OPERATIONAL COORDINATION: Establishing structure and plans for an anticipated contested cyber environment

Private sector entities often lead in developing cutting-edge technologies (e.g., AI, 5G/6G, Post-Quantum Cryptography). The government depends on this innovation to stay ahead of emerging threats and to inform policy and consensus standards development. Through reports shared with the public and government, the **Emerging Technologies Committee (ETC)** influences government understanding and action on cybersecurity risks. These contributions help shape best practices that protect both public and private interests. For example, in April, the ETC engaged with NIST to refine the core elements of the NIST Cyber AI Profile and how to align it with the existing NIST Cybersecurity Framework (CSF) and the AI Risk Management Framework (AI RMF). Through the Information and Communications Technology Supply Chain Risk Management Taskforce, they also published the *Supplier, Products, and Services Threat Evaluation Report (to include Artificial Intelligence Risks and Mitigations)*.[1]

The **Cybersecurity Committee** developed the consensus document, *Deploying Resource Public Key Infrastructure (RPKI): Steps for Prioritization and Implementation*,[2] as a follow-up to the *Roadmap to Enhancing Internet Routing Security, A Report by the White House Office of the National Cyber Director*. It is intended to help network operators of all types (service providers, enterprises, governments) understand the risks posed by Internet routing incidents, the benefits of mitigating the risks of such incidents through the use of the RPKI, and steps that can be taken to prioritize these mitigation efforts where needed.

Necessity of Agile Preparedness and Response

The private sector owns and operates much of the infrastructure deemed critical to national security. Companies in the communications sector play a vital role in identifying cyber threats and sharing intelligence. Information sharing in the communications sector between government and industry provides the best information to enable an agile response to the ever-increasing threats to both cybersecurity and national security. Collaborative forums (e.g., the CISA Joint Cyber Defense Collaborative and Network Security Information Exchange) demonstrate how private providers contribute to real-time threat mitigation and incident response and help test and strengthen resilience against disruption.

The **Infrastructure and 5G Committee** has a long history of industry collaboration with the Department of Homeland Security (DHS) regarding Position, Navigation, and Timing (PNT). This year, industry supported a DHS Tabletop Exercise (TTX) with small and mid-sized wireless carriers, demonstrating continued network availability, reliability, and resilience to PNT outages.

Throughout the year, the **Supply Chain Committee** briefed members and conducted outreach with the US Government on supply chain security topics, including engaging with the Department of Commerce's Bureau of Industry and Security's Office of Information and Communications Technology and Services on continued identification and mitigation of risks from certain modules in connected vehicles, and ongoing investigations into vulnerabilities in the supply chain of the growing data center industry.

Throughout 2025, the **Small and Mid-Size Business (SMB) Committee** kept committee members abreast of initiatives and developments at the DHS and other federal agencies. The committee also discussed cyber disruptions, weather disasters, and other emergency events in the context of how they impacted committee members and SMBs generally. The committee rounded out the year by soliciting committee members' views on event-driven advisories, response, guidance, and other information tailored to SMBs to help ensure federal advisories and other methods of communication account for SMBs.

The **Operational Coordination Committee** remained busy as ever in 2025 providing input on federal cyber and physical incident management structures and protecting major events by documenting how emergency services calls (e.g., 911) are handled for foreign visitors roaming in the US. The committee, through the Communications Information Sharing and Analysis Center, helped develop the Emergency Support Function (ESF) #2 – Communications spring workshop (a joint effort between government and industry), supported natural disaster related events with the Federal Communications Commission, collaborated with Japan on ICT information sharing and analysis best practices, and worked with the Department of War to plan for mission readiness in a contested environment.

Key conflict preparation activities:

- **US Cyber Command Cyberspace Partnership Conference**
- **Joint Staff war game**
- **Defense Critical Infrastructure (DCI) exercise planning**
- **Geographic assessments with DoW and DHS for DCI resilience**



Collaboration With Other Private Sector Organizations

In recognition of the tenuous road ahead, the private sector stepped up in 2025 to band together for security and resilience. Leading communications providers have established a formal forum for collaboration, bringing together the Chief Information Security Officers (CISOs) from the largest carriers in the United States and Canada. In the future, the group will also expand to include CISOs from other like-minded countries, further broadening its scope and influence. As a result, engagement and coordination at both the CISO and senior staff levels have significantly increased across the sector. Notably, the CISO forum directed the establishment of the Communications Cybersecurity ISAC (C2 ISAC); the new ISAC formally launched in September with a small cadre and is expected to begin operations and start to expand in 2026.

The interdependent nature of critical infrastructure requires cross-sector collaboration. The sector continued its established cross-sector partnerships in 2025, including leadership roles within the National Council of ISACs (NCI) where the sector contributed to projects such as developing shared best practices against cyber criminals, understanding risks related to undersea cables, promoting continuity of communications, and participation in other sector exercises. Building upon the legacy of the Tri-Sector Executive Working Group, the Alliance for Critical Infrastructure (ACI), launched as an industry-led council bringing together owners, operators, and industry representatives from the energy, communications, and finance sectors. ACI aims to facilitate collaboration and information sharing across these essential industries. By leveraging existing resources and expertise across sectors, ACI aims to protect vital infrastructure and provide a streamlining point of collaboration with government, especially in a time of crisis.

The Path Forward Contains Risks, Priorities, and Actions

Next year, the sector plans to deepen its partnership with the Office of National Cyber Director (ONCD), Department of War (DoW), and DHS to support national efforts to protect "Defense Critical Infrastructure"—the communications, energy, water, and transportation systems critical to US national defense missions. Additionally, the sector will continue internal coordination to share information and effective practices against nation-state adversaries.

In 2026 and beyond, the CSCC is anticipating working on efforts to address continuing risks through Post-Quantum Cryptography (PQC) readiness efforts with partners such as NIST and CISA. Similar work will continue regarding AI Risk Management such as guidance for securing AI models, using AI for defense, and AI supply chain security.

Public-private collaboration and information sharing is still in need of enhancement. We continue to see challenges in collaboration between federal agencies, which at times has placed the industry in the position of helping coordinate between multiple agencies. Congress can play an important role in driving more effective and sustained interagency collaboration.

ENDNOTES

1 *Supplier, Products, and Services Threat Evaluation Report (to include Artificial Intelligence Risks and Mitigations:* https://www.comms-scc.org/2025/07/11/supplier-products-and-services-threat-evaluation-report-to-include-artificial-intelligence-risks-and-mitigations/

2 *Deploying Resource Public Key Infrastructure (RPKI): Steps for Prioritization and Implementation*: https://www.comms-scc.org/2025/06/02/deploying-resource-public-key-infrastructure-rpki-steps-for-prioritization-and-implementation/

EXECUTIVE COMMITTEE

Officers & Liaisons

Robert Mayer, Chair (USTelecom – The Broadband Association)

Kathryn Condello, Vice Chair (Lumen) & NSTAC Liaison

Elizabeth Chernow, 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)

Traci Biswese (NCTA – The Internet & Television Association)

John Hunter (T-Mobile)

John Marinho (CTIA)

Christopher Oatway (Verizon)

Tamber Ray (NTCA – The Rural Broadband Association)

Allan Reiter (Nex-Tech)

Alana Scott (Ericsson)

Samuel Visner (Netcracker)

Larry Walke (National Association of Broadcasters)

STANDING COMMITTEES

Administrative Committee

Jessica Almond, Co-Chair (CableLabs)

Elizabeth Chernow, Co-Chair (Comcast)

Emily Murtaugh, Co-Chair (NCTA)

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 Committee

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)

Justin Perkins, Co-Chair (CTIA)

Alana Scott, Co-Chair (Ericsson)

Infrastructure and 5G/6G Committee

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.

Jessica Almond, Co-Chair (CableLabs)

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)

Strategy & Coordination Committee

Oversees policy considerations and CSCC priorities, providing strategic guidance to ensure alignment across working committees and supporting the Executive Committee in setting the Council's direction.

Christopher Oatway, Co-Chair (Verizon)

Jennifer Prime, Co-Chair (Cox)

Christopher Braccia, Cross-Committee Coordinator (USTelecom)

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

Anita Patankar-Stoll, Co-Chair (Verizon)

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
Comcast
Competitive Carriers Association
CompTIA
Consumer Technology Association
Cox Communications
CTIA – The Wireless Association
Cumulus Media
Ericsson
Fidium
Frontier
General Dynamics Information Technology
Hubbard Radio
Hughes Network
iconectiv
Internet Security Alliance
Iridium Communications
Juniper Networks
Lumen Technologies
National Association of Broadcasters
NCTA – The Internet & Television Association
NEC Corporation of America
Netcracker Technologies
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
TransUnion
Uniti
U.S. Cellular
USTelecom – The Broadband Association
Utilities Telecom Council
Verizon
WTA – Advocates for Rural Broadband

CONTACT:

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

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

COMMS-SCC.ORG

COMMUNICATIONS SECTOR COORDINATING COUNCIL