
# Communications Sector Coordinating Council 2022

## ADDRESSING TOMORROW'S THREATS TODAY

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

## ABOUT US

**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.**

## ADDRESSING COMPLEX CHALLENGES

Throughout 2021, CSCC members continued to show tenacity for maintaining and improving reliable and resilient communications networks in the face of a growing number of complex threats. As COVID-19 restrictions and the imperative to work from home and stay at home continue, there has been a greater exposure to cyber risk. Cybersecurity attacks continued to increase through 2021—both in terms of threat vectors, numbers, and consequences; just as climate change has increased the intensity and frequency of extreme weather. Additionally, the adoption and integration of Internet of Things (IoT) is creating a complex mesh of cyber-physical systems which expands attack surfaces.

*Increasing Threats, Vulnerabilities, Victims, and Consequences*

- **Average data breach costs rose 10% between 2020 and 2021**, from $3.86 million to $4.24 million, and **remote working and digital transformation due to the COVID-19 pandemic** increased the average cost of a data breach by **$1.07 million**.

  (IBM SECURITY, 2021)

- In 2021, **ransomware** attackers focused on approaches for impacts including **sophisticated supply chain attacks** with extended blast radiuses, double extortion, and Ransomware as a Service (RaaS). Ransomware accounts for 10% of all breaches—**which doubled in frequency in 2021**.

  (VERIZON, 2021)

- In the **first six months of 2021** alone, there was already **$590 million** in ransomware-related activity whereas there was only $416 million reported for all of 2020.

  (FEDERAL CRIMES ENFORCEMENT NETWORK (U.S. TREASURY), 2021)

- In 2021, **20 disastrous weather events** hit the United States, with losses exceeding **$1 billion each**. By contrast, the 1980-2021 annual average was 7.4 events, whereas the annual average for 2017-2021 was 17.2 events.

  (NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION, 2021)

- **31 billion IoT devices** are expected to flood the ecosystem by 2023. **IoT devices remain vulnerable** due to lack of physical hardening, insecure data storage and transfer, lack of visibility and device management, botnets, weak passcodes, insecure ecosystem interfaces, and AI-based attacks.

  (SECURITYSCORECARD, 2021)

## NEW PARTNERSHIPS

### *Joint Cyber Defense Collaborative*

CSCC members are collaborating with the Cybersecurity and Infrastructure Security Agency (CISA) in its new effort, the Joint Cyber Defense Collaborative (JCDC). The JCDC will bring together public and private sector entities to unify deliberate and crisis action planning while coordinating the integrated execution of these plans. Through the JCDC, launched in August 2021, partners from federal agencies, state, local, tribal, territorial (SLTT) governments, and the private sector are working together to promote national resilience by coordinating actions to identify, protect against, detect, and respond to malicious cyber activity targeting U.S. critical infrastructure or national interests. CSCC members AT&T, Lumen, and Verizon were among the initial JCDC industry partners at the launch of the effort along with the Department of Homeland Security, Department of Justice, U.S. Cyber Command, National Security Agency (NSA), Federal Bureau of Investigations, and Office of the Director of National Intelligence.

### *Enduring Security Framework*

Over the last year, the CSCC members have formalized and expanded their participation in the Enduring Security Framework (ESF) working group. The ESF is a public-private partnership led by CISA and the NSA along with the DoD, intelligence community, and industry partners. The working group is focused on understanding and responding to threats and risks to the security and stability of U.S. national security systems and critical infrastructure.

## NATIONAL SECURITY PRIORITIES

### *Securing the Supply Chain*

Supply chain risk management is a key component of cyber and physical security and is necessary to prevent and mitigate information, communications, and technology (ICT) vulnerabilities related to services and products. CSCC engages across federal agencies to promote concerted efforts and a consistent approach to supply chain risk management (SCRM). In 2021, the CSCC continued its efforts across multiple workstreams from briefing the White House on feedback from over 200 entities representing all five segments of the communications sector to the extended continued effort as co-lead of the DHS information and communications technology (ICT) SCRM task force and is preparing for more engagement in the coming year.

Major collaboration with government included Department of Commerce (National Telecommunications and Information Administration and National Institute of Standards and Technology), DoD, DHS, and the Federal Communications Commission. These are some examples of resources for which CSCC provided input: Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information; Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks; Vendor SCRM Template; The Minimum Elements for a Software Bill of Materials (SBOM); SBOM Myths vs. Facts; Framing Software Component Transparency: Establishing a Common SBOM (2nd Edition); SBOM Decision Points; and the Cybersecurity Maturity Model Certification.

## 5G

Wireless carriers are transitioning to the 5th generation of wireless technology (5G) at a record pace, and CSCC members are uniquely positioned to understand and mitigate security risks. Three years after initial launch, 5G networks are now available to more than 91% of Americans. Along with this rollout, the wireless industry has worked to ensure 5G is the most secure generation of wireless technology, with enhanced protections built in from the ground-up. Carriers continue to collaborate with each other and government to monitor, assess, and mitigate security threats, further demonstrating the industry's commitment to enhancing protections from cyberattacks.

CSCC members are uniquely positioned to understand and mitigate security risks. Major CSCC efforts and accomplishments include:

- Prepared for National Telecommunications and Information Administration (NTIA) National Strategy to Secure 5G Implementation Plan, and participated in Listening Sessions, which touched on topics such as standards, Open RAN, information sharing, and security.
- Partnered with CISA on mitigation efforts to ensure the opportunities of 5G are realized and engaged on the development and operationalization of CISA's Strategy.
- Worked with Department of Homeland Security Analytics Exchange Program (DHS AEP) to issue a report cataloging the Security Implications of 5G Technology.

In 2022, CSCC members continue to:

- Participate in the Federal Communication Commission's (FCC's) rechartered CSRIC VIII, focusing on 5G network and software security.
- Engage with DHS CISA and the Department of Defense on the development of 5G test beds.
- Focus on efforts to secure the supply chain.

### *Assessing Position, Navigation, and Timing Risk*

Positioning, Navigation, and Timing (PNT) is necessary for the functioning of the Nation's critical infrastructure and used for civil, commercial, and military use. The ubiquitous use of the Global Positioning Navigation (GPS) as the primary source of PNT information makes sectors vulnerable to adversaries seeking to cause harm by disrupting or manipulating GPS signal. PNT efforts are particularly critical in light of the November 2021 Russian test of its new anti-satellite technology and threat to attack NATOs 32 GPS satellites. In 2021, CSCC partnered in a DHS effort to strengthen PNT for critical infrastructure sectors, including a coordinated PNT vulnerability risk assessment for the Communications Sector. Based on input from the five segments, it was determined that the Communication Sector faces minimal risk to critical functions or general operations, even in the face of PNT disruptions or outages.

### *Climate Change, Sustainability, and Extreme Weather*

CSCC members are addressing the challenges of climate change while promoting innovation, efficiency, and advancing resilience and response to climate impacts. Many CSCC members are actively engaged, taking action to lower their greenhouse gas emissions while also providing solutions for customers to minimize carbon footprints by reducing the need for business travel. Providing high-speed, low-latency networks enables enhanced management of resources such as electricity, fuel, water, and raw materials. Additionally, CSCC members advocate for a strong private-sector role in wise management and use of resources, effective environmental stewardship, and greener growth through efforts such as off-the-record briefings with U.S. and international policymakers led by the International Chamber of Commerce and United States Council for International Business.

Extreme weather events are increasingly disrupting our nation's energy and transportation systems, threatening more frequent and longer-lasting power outages, fuel shortages, and service disruptions, with cascading impacts on communications assets and systems. In 2021, through the Communications Information Sharing and Analysis Center, (COMM-ISAC), CSCC members in collaboration with federal, state, and local government partners have also responded to a record number of natural disasters, including fires in the western U.S. and an extremely active Atlantic hurricane season—many of which occurred simultaneously.

## KEY LEGISLATIVE DEVELOPMENTS

CSCC members provided technical advice on a broad set of cybersecurity legislative proposals including regular engagement with Cyberspace Solarium Commission staff, Members of Congress, and congressional staff. In addition to testifying on incident response, CSCC members provided subject matter expertise on other issues including systemically important critical infrastructure, cybersecurity statistics, information sharing, 5G, and the global semiconductor shortage.

## INDUSTRY-LED EFFORTS

### *Multistakeholder Engagement*

Leveraging the CSCC's work over the last few years through multi-stakeholder venues such as the Council to Secure the Digital Economy (CSDE)[1], CSCC members have engaged on guidance for fighting botnets, developing secure IoT devices, and crisis response.

In March 2021, the CSDE released an updated International Botnet and IoT Security Guide, which lays out baseline practices that stakeholders should implement and highlights additional advanced capabilities that are presently available but underutilized. Building on 2019's C2 Consensus Baseline, CSDE released a 2021 Supplement and IoT Security Policy Principles, endorsed by 27 leading technology and security organizations, to inform governments about constructive paths to raise the market's expectations for and advance policy harmonization.

### *Semiconductor Shortage*

CSCC members have engaged on the impact of the cyber and national security impacts of the semiconductor shortage on the communications sector. According to an Access Partnership report, the communications sector accounted for up to half of all global semiconductor end-use in 2019, but in 2021 nearly three quarters of broadband operators reported challenges in obtaining equipment due to scarcity of the semiconductors that are core components of network equipment.

## ONGOING PARTNERSHIP EFFORTS

CSCC members draw on a years-long record of participation in multiple venues to keep government partners informed about cyber threats and intrusions, including the FCC's Disaster Information Reporting System and Network Outage Reporting System; voluntary cyber incident reporting relationships with the FBI and the Secret Service; compliance with the U.S. Securities and Exchange Commission requirement for publicly traded companies to disclose cyber incidents; and partnering with DHS across multiple venues to enhance the nation's cyber readiness.

### *NSTAC*

For over 30 years, the President's National Security Telecommunications Advisory Committee (NSTAC) has advised the U.S. government on national security and emergency preparedness challenges and items with the potential to impact the security, availability, and reliability of telecommunication services. The NSTAC's major areas of focus include strengthening national security, enhancing cybersecurity, maintaining global communications infrastructure, assuring communications for disaster response, and addressing critical infrastructure interdependencies and dependencies. CSCC members AT&T, Ericsson, Iridium, Lumen, and Neustar participate on the NSTAC, and AT&T serves as CSCC's liaison. In 2021, the NSTAC provided the following published documents for the President: Software Assurance in the ICT and Services Supply Chain, and Letter to the President on National Security and Emergency Preparedness Communications Priorities. One of the NSTAC's first efforts as a prominent model for trusted public/private partnerships included the recommendation for the creation of the National Coordinating Center as an operational arm of the NSTAC and as the Information Sharing and Analysis Center (ISAC) for the Communications Sector.



### *Comm-ISAC*

The Communications - Information Sharing and Analysis Center (ISAC) is the operational arm of the sector. Its goal is to avert or mitigate impacts upon telecommunications infrastructure so that communication networks remain operational, and it serves as a clearinghouse for physical and cyber alerts to the telecommunications industry. Steady state, we meet with our CISA Central partners and each other on a weekly basis, which has proven to substantially increase our overall response and recovery capabilities.

- **Contingency Plan for Core Network National Critical Function.** In collaboration with CISA and the Strategy, Policy, and Operations Program of the Homeland Security Operational Analysis Center federally funded research and development center (FFRDC), communication sector representatives developed a joint contingency plan for responding to and mitigating the impacts of a significant cyber incident affecting the communications core network infrastructure in the U.S. It outlines planning considerations for the federal government and communications sector coordination, information sharing, and support. This contingency plan was the first one developed and is intended to serve as a model for developing further plans covering other national critical functions.
- **Incident Response Planning and Exercises.** Responding to a cyber or physical incident requires extensive collaboration with partners in government, other industries, and global counterparts. CSCC members participate through the Comm-ISAC extensively in exercises to better understand interdependencies and mitigate risks.
  - **CyberStorm 2022.** Comm-ISAC industry members once again participated in the planning of CyberStorm 2022, providing subject matter expertise in the exercise control cell, and guidance on the master event scenario list (MESL).
  - **Clearpath VIII Exercise.** Several Comm-ISAC industry members once again actively participated in this Department of Energy led exercise, providing expertise and insightful information to our electricity sector colleagues, as reflected in the after action report. The communications industry has joined with the electric industry in a working group, led by DOE, to develop the criteria and MESL for Clearpath IV, which will take place in 2022.
  - **GridEx VI Participation.** Comm-ISAC industry members were once again invited to participate in planning through execution of GridEx VI, strengthening operational relationships with electric grid partners.
- **COVID-19 Temporary Medical Facilities Support.** Comm-ISAC industry members supplied secure communications to remote hospitals and other temporary facilities that were set up to handle the high number of COVID-19 cases.
- **NCC Charter.**
  - Worked closely with CISA's Integrated Operations Division (IOD) leadership to develop a new Charter, which defines the relationship between government and industry, and how the COMM-ISAC is used to make the nation more secure and resilient.
- **Other Activities.**
  - Coordinate with Federal Emergency Management Agency on Regional Emergency Communications.
  - Cultivate close relationships with ISACs of like-minded countries, notably Japan.

### *CSRIC VIII*

The Communications Security, Reliability, and Interoperability Council (CSRIC) makes recommendations to the FCC to promote the security, reliability, and resiliency of communications systems. CSCC members have figured prominently in leadership and contributory roles in each of the CSRIC and are once again participating in the newly recharted CSRIC VIII, which will convene through June 2023. Topics CSCC members will address are 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.

## ENDNOTES

1 The Council to Secure the Digital Economy (CSDE) brings together companies from across the ICT sector to combat increasingly sophisticated emerging cyber threats through collaborative actions. USTelecom and the Consumer Technology Association form the Secretariat for the CSDE. CSDE's membership consists of 15 global leaders and innovators representing different segments of the internet technology and communications ecosystem. See more at https://csde.org/

## REFERENCES


CTIA. (2021). *Industry Infographics*. Retrieved from cita.org: https://www.ctia.org/the-wireless-industry/infographics-library

Federal Crimes Enforcement Network (U.S. Treasury). (2021). *FinCEN Financial Trend Analysis: Ransomware Trends*. Retrieved from fincen.gov: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

IBM Security. (2021). *Cost of a Data Breach Report*. Retrieved from IBM.com: https://www.ibm.com/downloads/cas/OJDVQGRY

National Oceanic and Atmospheric Administration. (2021). *Billion-Dollar Weather and Climate Disasters*. Retrieved from National Centers for Environmental Information: https://www.ncdc.noaa.gov/billions/

SecurityScorecard. (2021). *7 Internet of Things Threats and Risks to Be Aware Of*. Retrieved from SecurityScorecard.com: https://securityscorecard.com/blog/internet-of-things-threats-and-risks

Verizon. (2021). *Verizon Data Breach Investigations Report*. Retrieved from Verizon.com: https://www.verizon.com/business/resources/reports/dbir/2021/


## EXECUTIVE COMMITTEE

**Robert Mayer,** Chair (USTelecom)

**Kathryn Condello,** Vice Chair (Lumen)

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

**Drew Morin,** Treasurer (T-Mobile)

**Joe Viens** (Charter) & Comms ISAC Liaison

**Chris Boyer** (AT&T) & NSTAC Liaison

**Jason Boswell** (Ericsson)

**John Marinho** (CTIA)

**Christopher Oatway** (Verizon)

**Jenny Prime** (Cox)

**Tamber Ray** (NTCA – The Rural Broadband Association)

**Matt Tooley** (NCTA – The Internet & Television Association)

**Larry Walke** (National Association of Broadcasters)

### *Administrative Committee*

**Rudy Brioché,** Chair (Comcast)

### *Finance Committee*

**Drew Morin,** Chair (T-Mobile)

## WORKING COMMITTEES

### *Cybersecurity Committee*

*Focuses on cyber initiatives and developments in supply chain; supports related activities and provides input to Executive Committee on appropriate policy considerations.*

**Paul Eisler,** Co-Chair (USTelecom)

**Tanya Kumar,** Co-Chair (T-Mobile)

**Matt Tooley,** Co-Chair (NCTA – The Internet & Television Association)

### *Information Sharing Committee*

*Coordinates sector input on information sharing issues and initiatives across government and industry landscape.*

**Chris Anderson,** Co-Chair (Lumen)

**Joe Viens,** Co-Chair (Charter)

### *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)

### *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 Travers,** Co-Chair (Lumen)

### *Small and Mid-size Business Committee*

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

**Chad Kliewer,** Co-Chair (Pioneer)

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

## CSCC MEMBER COMPANIES

3U Technologies
ACA Connects
Association for International Broadcasting
Alliance for Telecommunications Industry Solutions
AT&T*
CableLabs
Charter
Cincinnati Bell
Comcast
Competitive Carriers Association
CompTIA
Consolidated Communications
Consumer Technology Association
Cox Communications
CTIA - The Wireless Association
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
North American Broadcasters Association
Nsight
NTCA - The Rural Broadband Association
Nippon Telegraph and Telephone America
Pioneer Telephone Cooperative
Samsung
Satellite Industry Association
Telecommunications Industry Association
Telephone and Data Systems, Inc.
T-Mobile
U.S. Cellular
USTelecom - The Broadband Association
Utilities Technology Council
Verizon
Windstream
WTA – Advocates for Rural Broadband

**Participates on the President's National Security Telecommunications Advisory Committee.*

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

For more information visit www.comms-scc.org

**CONTACT:**

Chairperson: Robert Mayer, USTelecom
*rmayer@ustelecom.org*

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