COMMUNICATIONS SECTOR COORDINATING COUNCIL

Communications Sector Coordinating Council

ANNUAL REPORT 2023

Addressing Tomorrow's Threats Today

2022

was an eventful year that began under the shadow of Russia's impending war on Ukraine.

In 2022, threats continued at an unprecedented scale against sector members. Against a backdrop of a dynamic and rapidly evolving threat landscape with sophisticated and innovative cyber adversaries, the sector also faced increasingly uncertain geopolitical environment, extreme weather events, and the continued ramifications of COVID on people and systems. These global crises have many implications for national security and the security and resilience of our communications infrastructure. For example, Russia's war on Ukraine and threats against NATO allies are setting potential precedents on hybrid warfare (physical warfare combined with offensive cyber activities) and the targeting of assets of strategic economic and national importance as well as high value assets. CSCC members anticipate continued engagement on the implications of this environment throughout 2023, including enhancing the security of the Internet of Things (IoT), extreme weather resilience and changing climate adaptation, and addressing the malevolent use of domestic infrastructure.

- **Cyberattacks more than doubled against technology and telecommunications industries** because of greater reliance on digital environments and remote working.
- Organizations in the Americas experienced **DoS/DDoS and network manipulation attacks at a rate twice the global average.**
- **More than $2 billion in ransomware** was paid between 2019 and mid-2022, including more than $1 billion in 2021 alone.
- In 2022 (as of mid-October), the U.S. saw **15 weather/climate disaster events with losses exceeding $1 billion each**. These events included a drought, a flood, 10 severe storms, two tropical cyclones, and one wildfire.

Throughout the many efforts and activities undertaken by the CSCC in 2022, the following priorities were kept in mind.

ALIGNMENT. Because strategically aligned efforts have a better chance of success, the alignment of upcoming government initiatives has been a major focus for the CSCC. Alignment was a focus of CSCC comments on Cybersecurity Maturity Model 2.0, cyber incident reporting efforts (across international, federal [Cybersecurity and Infrastructure Security Agency (CISA), Federal Communications Commission (FCC), Securities and Exchange Commission (SEC)], and state entities), and systemically important critical infrastructure.

TRANSPARENCY. CSCC members advocated for and modeled a culture of transparency to customers and government entities on how we handle a wide range of security and resilience related issues. For example, in 2022 Congress required the National Institute of Standards and Technology (NIST) to establish an IoT Advisory and the Administration, CISA, and FCC continue to explore approaches to transparent IoT labeling and certification. CSCC members look forward to continuing to engage in the year ahead.

ADVANCEMENT. Through voluntary partnerships such as participation in the CISA Joint Cyber Defense Collaborative (JCDC), CSCC members illustrated the benefit of enhancing and improving intelligence and information sharing to evolve into joint operational collaboration.

INCLUSION. No matter their size or specialty, the CSCC encouraged efforts to ensure programs, protections, and related initiatives can be accomplished by small and medium-sized business (SMB) sector members. For example, the Small Broadband Provider ISAC promotes the resiliency and continuity of operation of small network operators across the United States. CyberShare experienced substantial growth this year and currently consists of nearly 90 small broadband providers. Working closely with industry partners, the federal government and other stakeholders, the Small Broadband Provider ISAC collects and disseminates threat information and facilitates communication between participants to help small broadband providers recognize, analyze, and respond to vulnerabilities, threats, and other risks. In 2022, the ISAC hosted an in-person Cybersecurity Summit featuring government and industry speakers in addition to multiple industry-wide webcasts on important cybersecurity topics.

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.*

Photo: David Vives, Unsplash.com

CSCC addresses the issues most important to protect the ecosystem for national security.

Supply chain resiliency. In 2022, CSCC members of the Enduring Security Framework (ESF) published a series on *Securing the Software Supply Chain,* releasing best practices guides for developers, suppliers, and customers. The Department of Homeland Security (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force advanced efforts for Hardware Bills of Materials, Small and Medium-sized Businesses, and Software Assurance.

"We approach [public-private partnerships] with humility [...] Certainly, we don't have all the answers, and this is not a problem that the government can solve. It's something we all collectively have to come together to solve—and with a sense of gratitude."

– JEN EASTERLY, DIRECTOR, CISA

Resiliency of emerging networks. 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 2022, ESF industry and government experts published an assessment of 5G network slicing, *Potential Threats to 5G Network Slicing*. The ESF also produced stakeholder guidance, *Open Radio Access Network Security Considerations*.

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 2022, CSCC members working through the Broadband Internet Technical Advisory Group (BITAG) published Security of the Internet's Routing Infrastructure report and filed an ex parte in response to the FCC's inquiry into Internet routing vulnerabilities.

Advancing consensus standards development. Cyber-attacks, increased geopolitical and economic competition, concerns with security, resiliency, interoperability, and other critical ICT issues have caused governments, industry, and users to focus more intently on how standards are developed and whether products and services are compliant with robust standards. In 2022, CSCC members undertook many efforts to advocate for and improve industry-led international consensus standards to drive a more vibrant and secure ICT supply chain, including sharing insights through the National Security Telecommunications Advisory Committee (NSTAC) to enhance U.S. competitiveness in international communications technology standards and continuing efforts through the ESF International Standards Group.

"Thanks to our existing public-private dialogue, NSA has been able to quickly identify and issue advisories on critical vulnerabilities and commercial software for the national security systems that could also potentially affect millions of users around the world."

– GEN. PAUL NAKASONE, COMMANDER, USCYBERCOM AND DIRECTOR, NSA

Partnership and collaboration between the private and public sectors are more important than ever to maintain business, government, and economic continuity, and to protect communications infrastructure and essential services.

The President's National Security Telecommunications Advisory Committee. The White House tasked the NSTAC with conducting a multi-phase study on "Enhancing Internet Resilience in 2021 and Beyond." The tasking directed NSTAC to focus on three key cybersecurity issues foundational to United States national security and emergency preparedness: I) *Software Assurance in the Information and Communications Technology and Services Supply Chain*, II) *Zero Trust and Trusted Identity Management*, and III) *NSTAC Report to the President on Information Technology and Operational Technology Convergence*. The first three phases of the tasking focus on developing recommendations to address each of these issues. In late 2022, the NSTAC focused on phase IV, which refines and builds on earlier key findings to produce an overarching report, *Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem*.

Communications Information Sharing and Analysis Center. At the beginning of 2022, the Comm-ISAC charter was signed after undergoing the first update in decades. It was the first step in further codifying the long-standing public-private partnership. Throughout the year, members developed standing operating procedures to help further organize the Comm-ISAC, and to help ensure both industry and CISA can operate together more effectively, while continuing to add value to all. Additionally, the Comm-ISAC drove sector resilience through planning and executing a sprint to improve PACE (Primary, Alternate, Contingency, Emergency) communications/coordination channels and established a sector-wide technological channel for the Comm-ISAC. Comm-ISAC partners shared information and responded to the Russian invasion of Ukraine and multiple climate events. The Comm-ISAC also engaged with international counterparts: Japanese counterparts interested in IoT certification, NIST activities, and developing partnerships with European ISACs and the U.S. National Council of ISACs; and Malaysian counterparts interested in capacity building.

Joint Cyber Defense Collaborative. The JCDC developed its Russia-Ukraine Cyber Defense Plan in early 2022 in response to the impending Russian invasion of Ukraine. CSCC Alliance partners in the JCDC contributed to the collaborative action framework for coordinating partner actions, building and enforcing resilience, and establishing channels and processes. From February through May 2022, the JCDC initiated the plan—leveraging technology channels to disseminate Russia-related information rapidly to members and partners, providing unclassified and classified briefings, and exercising additional plan elements through a snap Tabletop Exercise (TTX) based on previous Russian targeting of U.S.-based critical infrastructure.

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. Now in its eighth iteration, through June 2023, CSCC members once again figure prominently in leadership and contributory roles in all six working groups—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.

Collaboration across critical infrastructure sectors is essential to our shared security. In 2022, the private sector "Tri-Sector" group developed and hosted a Cyber Defense Exercise (CDX) between six companies from the communications, financial services, and electricity sectors. The CDX demonstrated the private sector's commitment to cybersecurity, and many government observers came to see the exercise and walked away deeply impressed. As a result, the CDX will expand and grow through the cross-sector public-private partnership facilitated by CISA, with the goal of adding capacity to critical infrastructure sectors facing more cybersecurity challenges as well as SMBs.

Engaging in long-term planning efforts impacting the security and resilience of communications infrastructure is a key activity of the SCC.

National Cybersecurity Strategy. CSCC members shared input with the Office of the National Cyber Director as it develops the Administration's National Cybersecurity Strategy (NCS) in coordination with the National Security Council.

Cross-Sector Cybersecurity Performance Goals and Sector Specific Goals. CSCC members engaged with CISA in the development of its Cybersecurity Performance Goals, a cross-sector common baseline system of performance goals. The CSCC will remain engaged as DHS continues its work to develop sector specific performance goals in 2023.

NIST Cybersecurity Framework Version 2.0. Communications sector stakeholders continue to champion the NIST Cybersecurity Framework, which has succeeded in helping organizations assess their cybersecurity risk for nearly a decade. CSCC members provided input as NIST works to develop Version 2.0, including through written comments and workshop participation, and look forward to working within an updated voluntary Framework that is compatible with other government efforts.

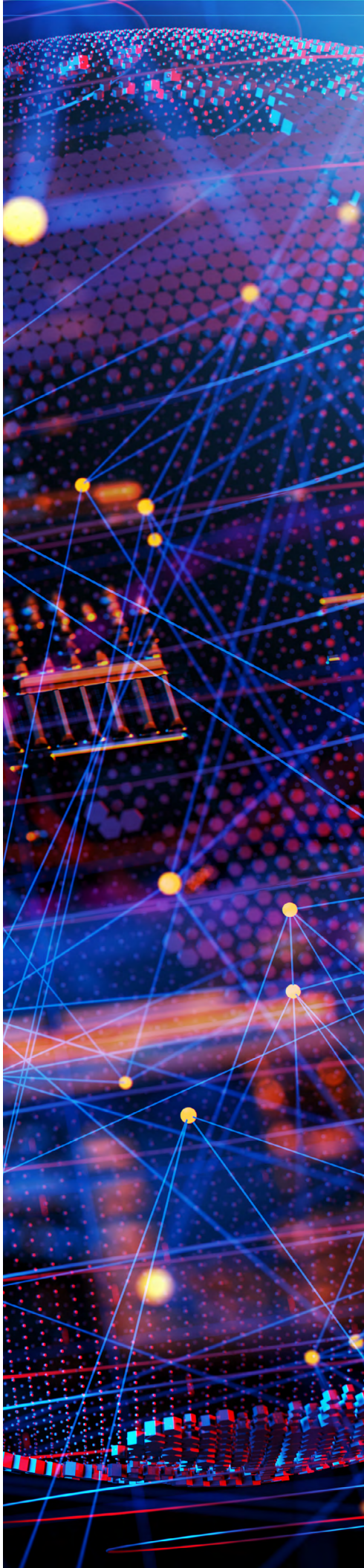
Cybersecurity in Subsidized Broadband Buildouts. Pursuant to NTIA's Broadband Equity, Access, and Deployment (BEAD) Program Notice of Funding Opportunity, CSCC members are working to ensure that subsidized broadband networks include foundational cybersecurity and supply chain security best practices.

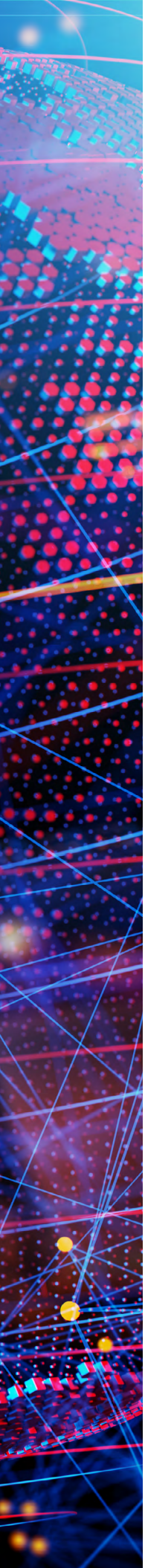
REFERENCES

Elementus Data Science Task Force, *Ransomware: A Technology Pandemic on the Brink*, rel. May 2022

National Oceanic and Atmospheric Administration. (2022). *Billion-Dollar Weather and Climate Disasters.* Retrieved from National Centers for Environmental Information: https://www.ncdc.noaa.gov/billions/

NTT Security Holdings, *2022 Global Threat Intelligence Report.* Retrieved from https://www.security.ntt/pdf/2022-global-threat-intelligence-report-v8.pdf





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)

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 is an active and fully engaged organization.

A 2022 survey of CSCC members found that 9 in 10 organizations find their CSCC participation valuable. The survey showed similarly high levels of satisfaction with the value of information that members receive from the CSCC, and with the organization's ability to build consensus. Additionally, responding members rated CSCC's:

Value to their organization ★★★★½

Value of information received on sectors issues ★★★★½

Frequency of communication ★★★★½

The CSCC is committed to adopting practices that raise the satisfaction of CSCC members in 2023.

CSCC members work closely with multiple federal government partners in a broad range of venues and on multiple workstreams.

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