IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

INTRODUCTION TO THE COMMUNICATIONS SECTOR RISK MANAGEMENT AGENCY

DEFEND TODAY,
SECURE TOMORROW

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an “enabling function” across all critical infrastructure sectors. Over the last 25 years, the Sector has evolved from being predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability.

COMMUNICATIONS SECTOR COLLABORATION, RESOURCES, AND TRAINING

The Cybersecurity and Infrastructure Security Agency (CISA) offers many resources to help owners and operators manage risks, improve security, and aid the implementation and execution of protective and response measures across the Communications Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted, additional information can be found on the CISA website at cisa.gov/communications-sector.

Collaboration

Sector Coordinating Council (SCC) and Working Groups convene regularly to share information and develop tools, guidelines, and products to address risks, vulnerabilities, and emerging issues to the Communications Sector. For information regarding the Communications SCC, visit comms-scc.org/.

Government Coordinating Council (GCC) and Working Groups composed of various federal departments, the GCC coordinates with the Cybersecurity and Infrastructure Security Agency (CISA) to identify and address shared priorities and initiatives that impact the Communications Sector. For information regarding the GCC, visit cisa.gov/communications-sector-council-charters-and-membership.

National Security Telecommunications Advisory Committee (NSTAC) helps the industry inform government decisions about National Security/Emergency Preparedness (NS/EP) communications. NSTAC provides the president with recommendations intended to ensure vital telecommunication connections are operational during times of crisis and to help the Federal Government maintain a reliable, secure, and resilient national communications posture. Visit cisa.gov/nstac.

Resources

Cybersecurity Framework is used to improve cyber resilience. CISA connects organizations with public and private sector resources that align to the Framework’s five function areas: identify, protect, detect, respond, and recover. Learn more at nist.gov/cyberframework.

Cyber Resource Hub is used to help agencies make data-informed risk decisions. CISA may conduct analysis of assessment data providing this information to partners. The Hub can help the broader cybersecurity community gain visibility with vulnerability trends, adversarial activities, and effective mitigations to implement for better protection of their networks. Learn more at cisa.gov/cyber-resource-hub.

Cybersecurity and Physical Security Convergence is guidance on converging cybersecurity and physical security functions to better position organizations to mitigate cyber-physical threats. To learn more, visit cisa.gov/publication/cybersecurity-and-physical-security-convergence.

Training

Cyber Storm is the Department of Homeland Security’s (DHS) flagship, biennial exercise series, which provides an opportunity for the Federal Government, state, local, tribal, and territorial (SLTT) organizations, and the private sector to address cyber incident response as a community. Now on its sixth iteration, each exercise in the series has simulated the discovery of, and response to, a coordinated C/I cyberattack.

Cyber Planning Support includes subject matter expert-run Cyber Planning Workshops, which are available to assist stakeholders with developing and revising integrated cyber plans.

Cyber Supply Chain Risk Management is a course created to educate the learner about cyber supply chain risk management (C-SCRM) and the role it plays within our society today. More specifically, the course teaches learners how to securely provision, analyze, oversee and govern, protect, and defend a supply chain.

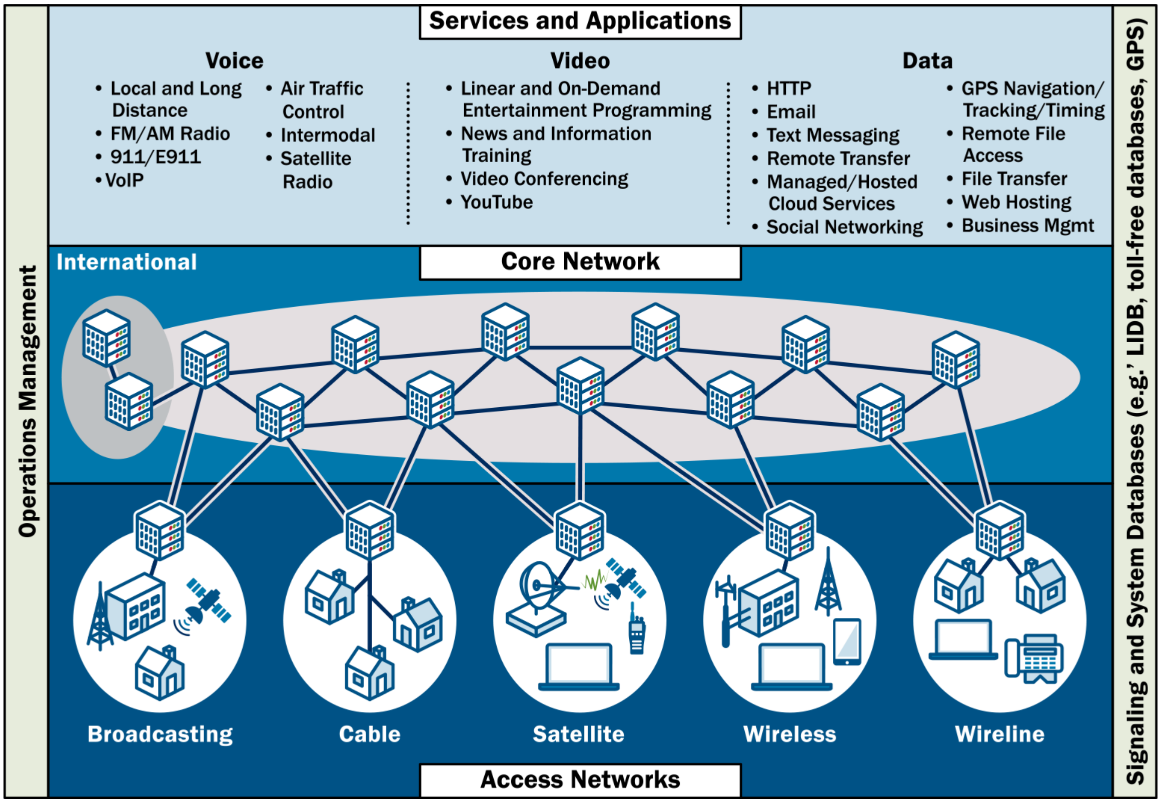
Critical Infrastructure Training information can be found at cisa.gov/critical-infrastructure-training. For more information on cyber exercises, contact ncciccustomerservice@hq.dhs.gov.

SECTOR PROFILE

The Communications Sector is both diverse and resilient with a strong, well-refined focus on risk management, long-established processes and procedures for network security, and rapid response and recovery under all hazards to assure the continued operation of vital communications. The infrastructure includes broadcasting, cable, satellite, wireless, and wireline capabilities, as well as the transport networks that support the Internet and other key information systems.

CRITICAL INFRASTRUCTURE SECURITY CONSIDERATIONS

As more devices connect to public communication networks, service firms can provide more types of device-specific services over those networks. The Communications Sector architecture model in the figure below serves as a representation of the collective infrastructure, which illustrates at least five major ways to access the numerous voice, video, and data services on the core network: broadcasting, cable, satellite, wireless, and wireline networks.



While the Communications Sector has few significant dependencies, other critical infrastructure sectors are dependent on the Communications Sector. As such, the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the Communications Sector to support its operations and associated day-to-day communication needs for corporate and organizational networks and services (e.g., internet connectivity, voice services, and video teleconferencing capabilities). Some sectors have even more significant dependencies on the Communications Sector beyond these routine operations.

FOR MORE INFORMATION ON THE COMMUNICATIONS SECTOR

Contact the Communications Sector Management Team at CommunicationsSector@cisa.dhs.gov or learn more at cisa.gov/sector-specific-agencies. For additional information about the Communications Sector, view the Communications Sector-Specific Plan at cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.