Cybersecurity

USTelecom is strengthening the arsenal of consumers, governments, and communications enterprises to combat cyber vulnerabilities and respond to rapidly evolving threats to our hyper-connected world.

The relentless pace of cyberattacks demands unprecedented industry and government collaboration to establish effective cyber risk management through shared information and best practices. USTelecom and its members work closely with government and industry to make sure the communications networks transporting information remain secure.

- Our partnerships within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the DHS National Risk Management Center promote greater coordination and collaboration across critical infrastructure sectors and increase education and awareness efforts related to cybersecurity threats, information sharing, and incident response.

- Our collaboration with the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) has resulted in the creation of practical frameworks for companies of all sizes to ensure systems and processes are current and secure.

USTelecom also leads:

ICT SUPPLY CHAIN RISK MANAGEMENT TASK FORCE ▶ USTelecom co-chairs DHS's new ICT Supply Chain Risk Management Task Force, a federal risk management effort to identify IT and communications supply chain risks and devise appropriate remedial measures. Given the complexities and overlapping interests of the communications supply chain, USTelecom encourages the federal government to evaluate and act upon threats using a consistent "whole of government" risk management methodology, informed by the intelligence and trade communities, and entities with the capabilities to make supply chain risk determinations.

THE COUNCIL TO SECURE THE DIGITAL ECONOMY ▶ USTelecom, along with the Information Technology Industry Council (ITI), launched the **Council to Secure the Digital Economy (CSDE)** to bring together companies from across the information technology and communications sectors to collaboratively combat increasingly sophisticated and emerging global cyber threats.

CSDE's **2018 International Anti-Botnet Guide** encourages collective and responsible action throughout diverse segments of the internet and communications ecosystem to tackle the problem of botnets across: (1) infrastructure, (2) software development, (3) devices and device systems, (4) home and small business systems installation, and (5) enterprises. The Administration has fully embraced this effort via NTIA's Botnet Roadmap, which incorporates CSDE's work. For more information, visit www.securingdigitaleconomy.org.

THE USTELECOM CYBERSECURITY TOOLKIT▶ USTelecom's Cybersecurity Toolkit is a comprehensive guide to navigating the complex world of cybersecurity. The toolkit includes the latest data on cybersecurity initiatives, including more than 350 links to cyber definitions, overviews and reports, as well as industry best practices and cybersecurity strategies. For more information, visit our website.