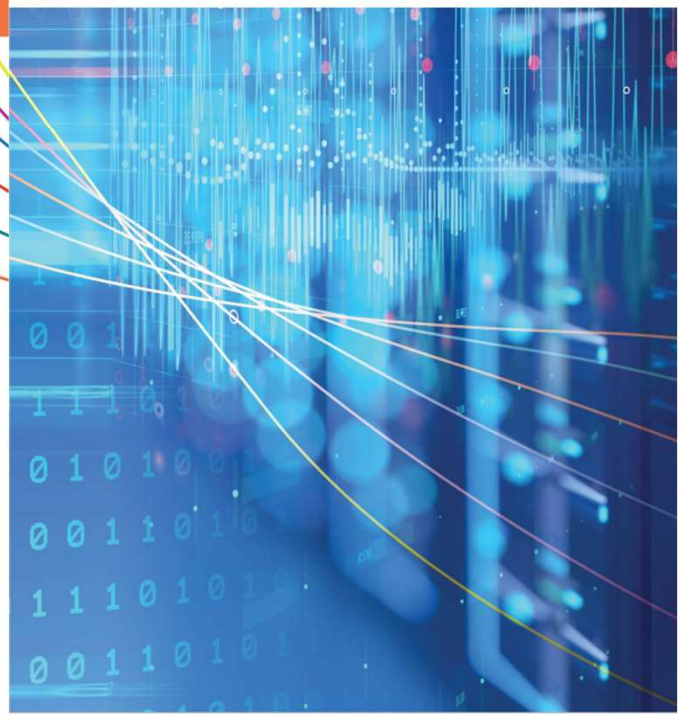
Understanding Cyber Threats to U.S. Critical Infrastructure



2022 OTA Accounting Conference
November 18, 2022

Presenter: Paul Eisler, USTelecom Senior Director Cybersecurity

USTELECOM
THE BROADBAND ASSOCIATION

What keeps policymakers up at night?

Example Scenarios

- DDoS Botnet Attack
- DDoS Server-based Attack
- Border Gateway Protocol (BGP) Hijacking
- Domain Name System (DNS) Hijacking
- Software Vulnerabilities: Open Source
- Software Vulnerabilities: Zero Day
- Hardware Vulnerabilities: Processor Architectures
- Injection of Malicious Code in Software and Hardware Components
- Destructive Malware
- Ransomware
- Advanced Persistent Threat (APT): Industrial Systems
- Cloud Provider Compromise

CSDE
Council to Secure the Digital Economy

USTELECOM THE BROADBAND ASSOCIATION | Consumer Technology Association

Federal Activity

- **Draft National Cyber Strategy**
- **NTIA Broadband Equity, Access, and Development Program (BEAD)**
  - First federal cybersecurity and supply chain risk management (SCRM) requirements for ISPs outside of a government contract
  - NIST Framework + EO 14028
- **CISA Performance Goals (National Security Memo 5)**
  - Cross-sector goals published
  - Work on sector-specific goals next year
- **CISA Incident Reporting Rulemaking**
  - CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act) requires owners and operators of critical infrastructure to report cyber incidents to CISA within 72 hours and ransom payments within 24 hours
- **SEC Cyber Disclosure**
- **FCC IoT Proceeding**
- **FCC BGP Proceeding**
- **NIST CSF 2.0**

Legislative Activity

- **Background / Solarium Commission**
- **Recent legislative proposals**
  - Mandatory Performance Goals
  - “Special Obligations of ISPs”
  - BGP/DNS security
  - Systemically Important Entities (SIE)

Questions/Discussion