Telecommunications Cybersecurity and Resilience Act

Senators Mark Warner (D-Virginia) and Ted Cruz (R-Texas)

Section 1. Short Title
Telecommunications Cybersecurity and Resilience Act

Section 2. Definitions
Defines terms used throughout the Act

Section 3. Telecommunications Cybersecurity Working Group
Establishes, within NTIA, a public-private advisory body called the Telecommunications Cybersecurity Working Group, tasked with developing Industry Best Practices, building a network of independent third-party assessors to certify implementation of those practices, and providing technical feedback and implementation guidance.

Requires NTIA to publish Industry Best Practices, implementation guidance, and assessor criteria; publish and submit to Congress the Working Group's bylaws, membership, and procedures; and publish an interagency memorandum of understanding among NTIA, CISA (as the CSRMA), NIST, and the FCC describing roles and coordination.

Section 4. Development of Industry Best Practices for Cybersecurity
Directs the Working Group, within 18 months of enactment and in consultation with NTIA, CISA, NIST, ODNI, ONCD, NSA, and the FCC, to develop and maintain voluntary Industry Best Practices and implementation guidance for telecommunications carriers, communications sector suppliers, and other supply chain participants. Those Industry Best Practices must be kept updated every two years or in response to a major incident or threat development.

The practices must:

1. Focus on identifying, responding to, mitigating, preventing, and remediating cybersecurity incidents and vulnerabilities;
2. Be risk-based and consistent with existing federal frameworks (e.g., the NIST cybersecurity framework, the NIST risk management framework, and guidance under executive order 14028);
3. Consider allied-nation cybersecurity requirements (NATO members, major non-NATO allies, or Five Eyes partners) for interoperability purposes;
4. Avoid duplicating existing risk-management processes; and
5. Reflect current threat intelligence and technology.

Industry Best Practices include, but are not limited to, timely application of security updates, decommissioning or mitigating unsupported network devices, configuration management practices aligned with the NIST Cybersecurity Framework 2.0, multi-factor authentication and identity/access-management measures, and other practices the Working Group establishes.

Section 5. Cybersecurity Certification Requirements for Eligible Entities
Directs the Working Group to develop, and the Assistant Secretary to approve, criteria for independent third-party cybersecurity assessors

Directs NTIA to establish an evaluation process, publish a list of eligible assessors, and set conditions for revoking or suspending an assessor's designation.
Prohibits an assessor owned or controlled by a telecommunications carrier from being designated as an eligible assessor.

Allows an eligible entity evaluated by an eligible assessor and issued a proposed certification to submit that certification to NTIA for approval, including the full assessment report, documentation of the practices evaluated, and required conflict-of-interest disclosures.

Provides that a certified entity is entitled to an affirmative defense in Federal or State court, and that an approved certification constitutes due care or reasonableness in mitigating, preventing, and remediating cybersecurity incidents, unless the entity acted with gross negligence or willful misconduct or did not materially implement and maintain the certified practices.

Preempts State or local laws imposing cybersecurity duties, standards, or liability inconsistent with the Act with respect to a certified entity.

Requires each approved certification to be valid for up to two years; authorizes revocation by NTIA if an assessor issues invalid or false certifications.

Prohibits retaliation against employees of an eligible assessor or a carrier

Authorizes NTIA to direct or commission an early reassessment of a certified entity, and to suspend its certification upon a written finding of credible evidence of material failure to implement or maintain the practices, pending completion of the reassessment.

Section 6. Reporting Requirements
Requires NTIA, in consultation with the Working Group, to submit an annual report to the relevant congressional committees and publish a public version covering development and updates to the practices, participation in certification, a summary of early reassessment activity, an assessment of adoption, and the overall effectiveness of the practices and certification regime.

Requires NTIA, in consultation with the Working Group to submit a report to Congress within 90 days of a substantial revision to the Industry Best Practices or a significant cybersecurity incident (as defined by PPD-41) affecting the telecommunications sector, including the Working Group's consensus views and recommendations.

Section 7. Rules of Construction

Nothing in the Act:
1. Grants new regulatory authority to any Federal agency, alters obligations or authorities under the Communications Act of 1934, the Secure and Trusted Communications Networks Act of 2019, or the Secure Equipment Act of 2021;
2. Prohibits the Working Group from consulting existing Federal advisory committees such as NSTAC, CSRIC, or the Commission's Technological Advisory Council;
3. Requires adoption of the Industry Best Practices or authorizes any regulatory requirement of adoption;

4. Displaces existing advisory councils or information-sharing agreements; or
5. Authorizes any Federal authority to supervise, direct, mandate, regulate, audit, or otherwise oversee carriers' or eligible entities' cybersecurity operations beyond what is expressly permitted for the voluntary best-practices and certification framework established by the Act.

Section 8. Severability
Provides that if any provision of the Act, or its application to any person or circumstance, is held unconstitutional, the remainder of the Act and its application to other persons or circumstances is unaffected.