McCAUL - WARNER COMMISSION
ON DIGITAL SECURITY

FINDINGS

- Digital security and communications technology and national security are inextricably linked.
- Technological innovation is critical to the U.S. economy and competitiveness.
- Digital security and communications technology (including encryption) protects critical infrastructure, financial systems, health records, online security, commercial transactions, government information, and personal privacy.
- Malicious actors can also use this technology to facilitate criminal activities.
- Terrorists and criminals are known to use digital security and communications technology to avoid detection.
- These beneficial technological advancements can also create challenges for law enforcement and national security.
- It is increasingly important that analysts, law enforcement, and policymakers understand this complicated digital landscape.
- The U.S. faces a difficult question of how to take advantage of privacy and security benefits of digital security and communications technology while minimizing risks posed by its abuse.
- No clear path forward exists despite years of dialogue between the tech sector, law enforcement, and national security professionals.
- Experts, practitioners, and relevant stakeholders must be brought together to address these issues and determine implications for all relevant fields.
- It is important to recognize that the communications marketplace is global and competitive.
- The two security interests require a forward thinking approach.

ESTABLISHMENT OF COMMISSION

The Commission is established to bring together leading experts to examine the intersection of technology and security and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.

In a report to Congress, the Commission will provide, at a minimum, assessments of:

- The issue of multiple security interests (public safety, privacy, national security, and communications and data protection) both now and in ten years.
- The economic and commercial value of cryptography and digital security and communications technology.
- The benefits of cryptography and digital security and communications technology to national security and crime prevention.
- The role of cryptography and digital security and communications technology in protecting the privacy and civil liberties of Americans.
- The effects the use of cryptography and other digital security and communications technology has on law enforcement and counterterrorism.
- The costs of weakening cryptography and digital security and communications technology standards. International laws, standards, and practices for legal access to communications and data protected by cryptography and digital security and communications technology.

McCAUL - WARNER COMMISSION
ON DIGITAL SECURITY

The Commission's report will also include recommendations for policy and practice, and may include recommendations for legislation, regarding:

- Methods to take advantage of the benefits of digital security and communications technology while mitigating the risk of abuse by bad actors.
- The tools, training, and resources that could be utilized by law enforcement and national security agencies to adapt to the new digital landscape.
- Cooperation between the government and private sector to work together to impede terrorists' use of digital security and communications technology to mobilize, facilitate, and carry out attacks.
- Any revisions to current law regarding wiretaps and warrants for digital data, while preserving privacy and market competitiveness.
- Proposed changes to procedures for obtaining warrants to increase efficiency and cost effectiveness for the government, tech companies, and service providers.
- Steps the U.S. can take to lead the development of international standards for digital evidence for criminal investigations, including reforming the mutual legal assistance treaty (MLAT) process.

COMPOSITION OF COMMISSION

- There will be ***16 total commissioners.***
- The Speaker of the House and Senate Majority Leader will appoint eight commissioners (one from each field below), including one Chairman.
- The House Minority Leader and the Senate Minority Leader will appoint eight commissioners (one from each field below), including one Vice Chairman.
- The Majority and Minority shall appoint U.S. citizens with experience from each of the following fields:
    - ***Cryptography***
    - ***Global commerce and economics***
    - ***Federal law enforcement***
    - ***State and local law enforcement***
    - ***Consumer-facing technology sector***
    - ***Enterprise technology sector***
    - ***Intelligence community***
    - ***Privacy and civil liberties community***
- The President may appoint one ex officio individual to serve in a non-voting capacity.

Staffing

- The Chairman and Vice Chairman shall jointly appoint and fix the compensation of an executive director and other necessary staff.
- Federal agencies and departments shall cooperate expeditiously with the Commission in providing security clearances to commissioners and staff.
- The Commission is authorized to procure services of detailees, experts, and consultants.
- The Commission may accept voluntary and uncompensated services.

McCAUL - WARNER COMMISSION
ON DIGITAL SECURITY

TIMELINE

- Commissioners must be appointed within 30 days of enactment (except for the ex officio).
- The Commission shall hold its first meeting within 60 days of enactment.
- The interim report is due within 6 months of the initial meeting.
- The final report is due within 12 months of the initial meeting.
- The Commission terminates within 60 days after the final report.

PROCEDURES & POWERS

Rules
- The Commission may establish rules to conduct its business.

Hearing
- The Commission may hold hearings, take testimony, collect information, and require witnesses, as well as the production of documents, as it determines advisable.
- Commission may conduct public and private hearings, as long as conducted to protect information provided to or developed for or by the Commission.

Subpoena Authority
- A subpoena for information materially relevant to the duties of the Commission requires an affirmative vote of 12 of 16 members of Commission.

Receipt & Handling of Information
- The Commission is authorized to secure information directly from any executive branch entity.
- Sensitive or proprietary information shall only be received, handled, and stored by members and staff of the Commission consistent with all applicable statutes, regulations, and Executive orders.
- Information obtained by members and staff of the Commission may not be revealed or disseminated outside the Commission absent approval from a majority of the members.

Reports
- The interim report and final report must be approved by 11 of 16 commissioners.
- Reports may include dissenting views.
- Reports are to be public, but may include a classified annex.

Funding
- No additional funds are authorized to be appropriated; only existing funds shall be used.
- Upon termination of the Commission, remaining funds shall be returned to the general fund of the Treasury for the purpose of deficit reduction.