Additional Information on National Commission on Digital Security

Composition of the Commission

Two commissioners will be selected 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 Speaker of the House and Senate Majority Leader will appoint eight commissioners, one from each field, including a Chairman. The House Minority Leader and the Senate Minority Leader will appoint eight commissioners, one from each field, including one Vice Chairman.

In addition, the President may appoint one ex officio individual to serve on the Commission in a non-voting capacity.

Reporting

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.

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.

The Commission will issue an interim report within 6 months, and a final report within 12 months.

###