1 New Orchard Road
Armonk, NY 10540-1722

EXECUTIVE SUMMARY for IBM Response on "Current and Future States of Cybersecurity in the Digital Economy"

As digital technology increasingly underpins business, government, and personal interactions, a rapid parallel evolution of cybercrime has become one of society's biggest problems.

The United Nations has reported that 80 percent of cyberattacks originate from highly organized crime rings, operating with the same level of collaboration as legitimate businesses. Global networks of thieves are working together to steal intellectual capital, control free speech and embezzle money. While nation state cyber espionage and terrorism receive ample media attention and remain valid concerns, the ascent, size and sophistication of cybercrime rings, and the threat they pose to public and private organizations, is also a significant societal issue, which needs to be addressed through a combination of cybersecurity innovation, technology, and policy.

To keep pace, IBM has been at the forefront of cybersecurity research and innovation in intelligent systems that detect and prevent threats. IBM proposes that cybersecurity needs to quickly evolve in two areas – the continued development and evolution of security intelligence systems, and, equally important, a much faster jump to a massive collaboration across the public and private sector, combining forces, data and know-how.

In response to the Commission's request for information on the state of cybersecurity, IBM first presents an overview of cognitive computing and blockchain, innovations that combat escalating organized cybercrime.

IBM is bringing cognitive computing to the war on cybercrime later this year. Called Watson for cyber security, this technology sorts through, analyzes and understands massive amounts of structured and unstructured security data that can overwhelm security professionals. Cognitive technology understands the nuances of imprecise language and threat data from the internet, makes connections between them, and offers remediation actions and strategies, all with the necessary speed to stay ahead of advanced threats.

Blockchain technology can help substantially reduce fraud and cybercrime as businesses digitally record transactions – whether they are currency exchange, supply chain, or other types of transactions between parties. As IBM recently testified before the Commission, there are four areas where government and industry should work together on Blockchain: proof of identity, data provenance, secure transaction processing, and intelligence sharing.

To address specific issues of concern to the Commission, IBM's submission will also provide insight into two areas where IBM has extensive experience and proficiency: the cybersecurity of the internet of things and critical infrastructure.

At IBM, the technology we provide for our clients' and our own digital transformation is underpinned by a security program powered by expertise and innovation that is quickly evolving to outthink cybercriminals. Only when private and public organizations work together to share this expertise and intelligence will we gain an effective cybersecurity posture.