**G-7 Finance Ministers and Central Bank Governors**
**Press Release**

Washington, DC
October 2017

Cyber incidents are increasing in scale and sophistication, and improving the cybersecurity of the financial sector remains a critical objective for G-7 countries. The G-7 Cyber Expert Group ('CEG') continues to facilitate coordination across members and develop a G-7 view on best practices for cybersecurity in the finance sector. Last year, we published the *Fundamental Elements of Cybersecurity for the Financial Sector*, a set of non-binding elements which encapsulate effective practices in cybersecurity for public and private financial-sector entities.

Today we publish the *Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector*. The guidance provides institutions with a set of outcomes which demonstrate good cybersecurity practices, including: embedding of cybersecurity considerations into organizational decision-making; acknowledgment that technological disruptions will occur; adaptation to changing cyber risks; creation of a good cybersecurity culture.

The *Fundamental Elements for Effective Assessment* also set out five non-prescriptive, high-level process components for organizations to use when assessing their level of cybersecurity. These cover: (1) setting clear goals for cyber assessments; (2) establishing measurable expectations; (3) using a diverse range of tools; (4) clearly reporting findings and remedial actions; (5) ensuring that assessments are reliable and fair.

While legally non-binding, the *Fundamental Elements for Effective Assessment* set out a clear G-7 view of what effective practice for assessing cybersecurity looks like, which can be applied by financial institutions and authorities alike. The guidance is designed to be tailored to different jurisdictions, and to firms of different sizes and levels of maturity.

Building on the Bari Communiqué of May 2017, the CEG continues to work on third party risks and cross-sector coordination. In addition, the CEG will develop a set of fundamental elements for threat-led penetration testing, and proposals for cross-border cyber crisis simulation exercises involving G-7 financial authorities.